PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-242438
(43)Date of publication of application : 17.09.1996

(51)Int.Cl. H04N 7/167
G11B 20/10
H04L 9/18

(21)Application number : 07-308004
(22)Date of filing : 27.11.1995

(71)Applicant : LG ELECTRON INC
(72)Inventor : PARK TAE JOON

(30)Priority
Priority number : 94 9431364 Priority date : 26.11.1994 Priority country : KR

(54) METHOD AND DEVICE FOR ILLEGAL VIEWING/COPYING PREVENTION OF DIGITAL VIDEO SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illegal viewing and copying by transmitting a scrambled bit stream and the encrypted key used for the scrambling through mutually different pathsand descrambling the bit stream after decrypting the encrypted key with a smart card.
SOLUTION: A demodulation and error correction part 1 performs demodulation and RS decoding for an analog broadcast signal. An ATV decoder 2 descrambles the output of the correction part 1 according to descrambling information. A copying preventive process part 4on the other handseparates a scrambled recording signal into a bit stream and a key streamand encrypts the key stream. Then the smart card 3 decrypts the encrypted key stream separated by the process part 4 and the index code of the ATV decoder 2 and outputs descrambled information KS to the decoder 2. Thereforeauthentication and key exchange are performed automatically to prevent illegal viewing and copying.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]

[Claim 1]A distinction stage which distinguishes whether scramble (scramble) of the data inputted was carried outIf distinguished from data by which scramble was carried out in said distinction stageafter dividing into a bit stream and a key stream said data by which scramble was carried outDecode a separated key streamdecipher key informationand descrambling (descramble) of said separated bit stream is carried out according to key informationIf distinguished from a regeneration stage displayed in a display deviceand data by which scramble was carried out in said distinction stageAccording to record or copying moderecord on a recording medium by data status with which a bit stream and a key stream were mixed and by which scramble was carried outorA recording level which is mixed with a bit stream and recorded on a recording medium after dividing into a bit stream and a key stream data by which scramble was carried out and enciphering a separated key streamIf distinguished from data by which scramble was carried out in said distinction stageafter dividing into a bit stream and a key stream data by which scramble was carried outDecrypt a key stream separated according to "PPC" mode or "backup copy (Back-up Copy)" mode to key information by the side of recordand transmitorIllegal viewing and listening and a copy prevention method of a digital video system consisting of a transmission stage of decrypting a separated key stream twice and transmitting it to own key information and key information by the side of recordand being able to perform simultaneous or selectively said regeneration stagea recording leveland a transmission stage.

[Claim 2]Illegal viewing and listening and a copy prevention method of the digital video system according to claim 1 if distinguished from data by which scramble is not carried out in said distinction stagewherein data by which scramble is not carried out will not apply illegal viewing and listening and a copy preventing function.

[Claim 3]Illegal viewing and listening and a copy prevention method of the digital video system according to claim 1wherein said regeneration stage decrypts a separated key stream with a decryption algorithm to an MPEG bit stream and deciphers key information.

[Claim 4]The 1st step where copying operation of said recording level enciphers a key stream to own key informationThe 2nd step that distinguishes whether a key stream enciphered in the 1st step is in "PPC" modeor it is in "backup copy" modeIf distinguished from "PPC" mode in said 2nd stepafter enciphering to key information by the side of record of a key stream decrypted and transmitted to key information by the side of recordThe 3rd step that is inserted in a position corresponding to an index codeand is recorded like a bit streamIf distinguished from "backup copy" mode in said 2nd stepit will encipher to key information by the side of record of a key stream decrypted and transmitted to own key information and key information by the side of recordIllegal viewing and listening and a copy prevention method of the digital video system according to claim 1 inserting in a position corresponding to an index

codeand consisting of the 4th step recorded like a bit stream after decrypting to key information on the self.

[Claim 5]The 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after said 3rd-step "PPC" mode operation separates a bit stream and a key streamThe 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record after enciphering to own key informationAfter enciphering a key stream transmitted in said 2nd transmission stage to key information by the side of record corresponding to an index codeIllegal viewing and listening and a copy prevention method of the digital video system according to claim 4 consisting of a recording level which is mixed to a bit stream transmitted in said 1st transmission stageand is recorded on a recording medium.

[Claim 6]If it reproduces by completing record by said recording levelafter dividing a reproduced bit stream (S_{KS}(BS)+E^{G} (KS)) into a bit stream (S_{KS} (BS)) and a key stream (E^{G} (KS))A separation stage which inserts the index code IDX in a portion from which a key stream (E^{G} (KS)) was separatedAn encryption stage which enciphers a key stream (E^{G} (KS)) separated in said separation stage to own key informationA decipherment stage which deciphers key information by decrypting a key stream enciphered in said encryption stage to own key information and an MPEG bit streamIllegal viewing and listening and a copy prevention method of the digital video system according to claim 5 including a decryption stage which descrambles said separated bit stream (S_{KS} (BS)) based on key information deciphered in said decipherment stage.

[Claim 7]Said 4th-step "backup copy" mode operationThe 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after separating a bit stream and a key streamThe 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record of an enciphered key streamand own key information after enciphering to own key informationA key stream transmitted in said 2nd transmission stage is corresponded to an index codeIllegal viewing and listening and a copy prevention method of the digital video system according to claim 4 mixing to a bit stream transmitted in said 1st transmission stageand consisting of a recording level recorded on a recording medium after enciphering to key information by the side of record.

[Claim 8]If it reproduces by completing record by said recording levela reproduced bit stream (S_{KS}(BS)+D^{SC}_{AK} [E^{G} (KS)])After separating a bit stream (S_{KS} (BS)) and a key stream (D^{SC}_{AK} [E^{G} (KS)])A separation stage which inserts the index code IDX in a portion from which a key stream (D^{SC}_{AK} [E^{G} (KS)]) was separatedIn an encryption stage which enciphers a key stream (D^{SC}_{AK} [E^{G} (KS)]) separated in said separation stage to own key informationand said encryption stageBy decrypting a key stream enciphered twice to own key information and an MPEG bit streamIllegal viewing and

listening and a copy prevention method of the digital video system according to claim 7 including a decipherment stage which deciphers key informationand a decryption stage which descrambles a separated bit stream (S_{KS} (BS)) based on key information deciphered in said decipherment stage.

[Claim 9]If data by which scramble was carried out is inputtedafter dividing into a bit stream and a key stream said data by which scramble was carried outDecode a separated key streamdecipher key informationand said separated bit stream is descrambled based on deciphered key informationBy a regeneration stage displayed in a display deviceand data status with which a bit stream and a key stream were mixed when data by which scramble was carried out was inputted and by which scramble was carried out. Illegal viewing and listening and a copy prevention method of a digital video system consisting of a recording level recorded on a recording mediumand being able to perform said regeneration stage and a recording level simultaneous or selectively.

[Claim 10]It is the key information which said regeneration stage decoded a separated key stream with a decryption algorithm to an MPEG bit streamdeciphered key informationand was decipheredIllegal viewing and listening and a copy prevention method of the digital video system according to claim 9 distinguishing a descrambling method.

[Claim 11]If it reproduces by completing record by said recording levelafter dividing a reproduced bit stream (S_{KS}(BS)+E^G (KS)) into a bit stream (S_{KS} (BS)) and a key stream (E^G (KS))A separation stage which inserts the index code IDX in a portion from which a key stream (E^G (KS)) was separatedOwn key information is received in a key stream (E^G (KS)) separated in said separation stageBy decrypting a key stream enciphered twice to own key information and an MPEG bit stream in an encryption stage enciphered by an encryption algorithmand said encryption stageBased on key information deciphered in a decipherment stage which deciphers key informationand said decipherment stagesaid separated bit stream (S_{KS} (BS)) is descrambledIllegal viewing and listening and a copy prevention method of the digital video system according to claim 9 including a decryption stage displayed in a display device.

[Claim 12]If a key stream enciphered to own key information at the time of a copy is transmittedA distinction stage which distinguishes whether it is in "backup copy" modeor it is in "PPC" modeThe 1st transmission stage of decrypting and transmitting said key stream to key information by the side of record if distinguished from the [PPC" mode in said distinction stageAfter enciphering to key information by the side of record of a key stream transmitted in said 1st transmission stagean enciphered key stream is inserted in a position corresponding to an index codeIf distinguished from "backup copy" mode in the 1st recording level recorded on a recording medium like a bit streamand said distinction stageThe 2nd transmission stage of decrypting a key stream twice and transmitting it to own key information and key information by the side of recordAfter enciphering a key stream transmitted in said 2nd transmission

stage to key information by the side of recordIllegal viewing and listening and a copy prevention method of a digital video system which are characterized by the 2nd recording level that inserts an enciphered key stream in a position corresponding to an index codeand is recorded on a recording medium like a bit streamand a thing** and others.

[Claim 13]Illegal viewing and listening and a copy prevention method of the digital video system according to claim 12 transmitting it after said 1st transmission stage decrypts a key stream enciphered to the own key information Ak to the own key information Ak and decrypts it to key information aluminum by the side of record further.

[Claim 14]Said 2nd transmission stage a key stream enciphered to the own key information AkIllegal viewing and listening and a copy prevention method of the digital video system according to claim 12 transmitting after decrypting twice to the own key information Ak and decrypting to key information aluminum by the side of record further.

[Claim 15]If a key stream (E^{G} (KS)) is detected at the time of reproduction of a recording mediumit will distinguish from the "PPC" recording mediumAfter enciphering a key stream to own key informationdecode for own key information and key information is decipheredA "PPC" mode reproduction stage which descrambles a bit stream using key information and an index code which were decipheredIf a key stream (D^{SC}_{AK} [E^{G} (KS)]) decrypted to own key information at the time of reproduction of a recording medium is detectedAfter distinguishing from a "backup copy" recording medium and enciphering twice to key information by the side of self and recordIllegal viewing and listening and a copy prevention method of a digital video system decoding for own key informationdeciphering key informationand consisting of deciphered key information and a "backup copy" mode reproduction stage which descrambles a bit stream using an index code.

[Claim 16]A recovery and an error correction means which carry out the strange recovery of the analog broadcasting signaland carry out RS decodingAfter dividing into a bit stream and a key stream a record signal which transmits said recovery and an output of an error correction means to record/playback equipmentand is reproduced with its record/playback equipment and by which scramble was carried outA copy preventing process means to encipher a separated key streamand a decoder means to descramble a bit stream outputted from said recovery and an error correction meansor a copy preventing process means based on descrambling informationIllegal viewing and listening and a copy arrester of a digital video system having decoded a key stream enciphered by said copy preventing process meansand constituting from a smart means to output to said decoder means as descrambling information.

[Claim 17]A decoder means by which said recovery and an error correction means were connected is connected to a smart meansBy decoding a key stream of said

decoder means for own key information with said smart cardand outputting descrambling information to said decoder meansIllegal viewing and listening and a copy arrester of the digital video system according to claim 16 constituting so that an illegal viewing-and-listening preventing function may be performed.
[Claim 18]Illegal viewing and listening and a copy arrester of the digital video system according to claim 16 recording only after connecting to digital recording/playback equipment a copy preventing process means by which said recovery and an error correction means were connected.
[Claim 19]While connecting with a smart carda key stream line of a copy prevention means where said digital recording/playback equipment were connectedConnect a bit stream line to a decoder meansand said copy preventing process means and a decoder means are connectedWhen said smart card decodes a key stream of said copy preventing process means corresponding to an index code of said decoder means for own key information and outputs to said decoder means. Illegal viewing and listening and a copy arrester of the digital video system according to claim 16 preventing illegal reproduction.
[Claim 20]Said copy preventing process means enciphers a key stream separated from regenerative data of digital recording/playback equipment at the time of recording-medium reproduction in "PPC" mode for own key information. Illegal viewing and listening and a copy arrester of the digital video system according to claim 19 transmitting to a smart card.
[Claim 21]Said copy preventing process means enciphers twice a key stream separated from regenerative data of digital recording/playback equipment at the time of reproduction medium reproduction in "backup copy" mode for own key informationand it transmits to a smart cardIllegal viewing and listening and a copy arrester of the digital video system according to claim 19 by which it is characterized.
[Claim 22]RAM which memorizes key information that said copy preventing process means is peculiar to a smart cardAn algorithm storage memory which stores an encryption algorithmClaim 16 consisting of a processor which executes an enciphered program of said algorithm storage memory for key information on said RAM18 or a digital video system indicated to either of Claim 19and a copy arrester.
[Claim 23]The 1st algorithm storage memory in which said smart card stores a decryption algorithm program for bit SUTORIMUThe 2nd algorithm storage memory which stores an own decryption algorithm programIllegal viewing and listening and a copy arrester of a digital video system given in either Claim 16 constituting from a ROM which stores own key informationand RAM which carries out temporary storage of the key information on other smart cards17 or Claim 19.
[Claim 24]A 1st copy preventing process means to encipher a separated key stream after dividing regenerative data of the 1st digital recording / playback equipment into a bit stream and a key streamThe 1st and 2nd smart card that decrypts a key stream enciphered by said 1st copy preventing process means to own key information and

key information by the side of recordAfter enciphering a key stream of said 1st smart card transmitted via said 2nd smart card for own key informationwith a bit stream from which an enciphered key stream was separated. A 2nd copy preventing process means to output to the 2nd digital recording / playback equipmentand to record on a recording mediumillegal viewing and listening of a digital video system ** constitutingand a copy arrester.

[Claim 25]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24 transmitting it to the 1st smart card after said 1st copy preventing process means enciphers a key stream to the own key information Ak.

[Claim 26]When said 1st smart card is in "PPC" modeafter decrypting a key stream of the 1st copy preventing process means to own key information and key information by the side of recordIllegal viewing and listening and a copy arrester of the digital video system according to claim 24 transmitting to the 2nd smart card.

[Claim 27]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24 mixing it with a bit stream of the 1st copy preventing process means after said 2nd copy preventing process means enciphers a key stream transmitted with the 2nd smart card to own key information aluminum.

[Claim 28]When said 1st smart card is in "backup copy" modeIllegal viewing and listening and a copy arrester of the digital video system according to claim 24 which are characterized by decoding to key information by the side of record after decoding a key stream of the 1st copy preventing process means twice to own key information.

[Claim 29]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24wherein said 2nd copy preventing process means enciphers a key stream transmitted from the 2nd smart card to own key information and mixes the enciphered key stream with a bit stream.

[Claim 30]Illegal viewing and listening and a copy arrester of the digital video system according to claim 24 characterized by comprising the following.

RAM which stores key information that said 1st and 2nd copy preventing process means is peculiar to a smart card.

A processor which executes an enciphered program of said algorithm storage memory using an algorithm storage memory which stores an encryption algorithmand key information on said RAM.

[Claim 31]The 1st algorithm storage memory in which said 1st and 2nd smart card stores a decryption algorithm program for a bit streamIllegal viewing and listening and a copy arrester of the digital video system according to claim 24 constituting from a 2nd algorithm storage memory which stores an own decryption algorithm programa ROM which stores own key informationand RAM which carries out temporary storage of other smart key information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to illegal viewing and listening of a digital video systemand copy prevention art. By decoding the key stream separated by introducing especially a smart cardand setting up a descrambling methodit is related with illegal viewing-and-listening / copy prevention method and the device of a digital video system which prevent illegal viewing and listening and a copy of an unapproved user.
[0002]
[Description of the Prior Art]Concern is concentrating on the embodiment of a Conditional Access (henceforth CA) system by the common digital video system for the prevention from illegal viewing and listening.
[0003]It is formal by broadcasting such a CA system with the gestalt by which scramble was carried out in the broadcasting signal by charged channelssuch as a cable TV and satellite broadcastingand only the user who paid money enables it to view and listen to a broadcast program to ** via descrambling. For examplethe satellite broadcasting receiver or the GrandAllinace (henceforth GA) system of a U.S. ATV standard has a function for supporting CA.
Scrambling / descrambling device used for satellite broadcasting like the video code (Video Cipher) of GI were also already daily-use-ized.

[0004]The scrambling system for a common CA system is a video code (Video Cipher) system of GI.
If this carries out the scramble of the television signal transmitted to a regular member's descrambler by a charged TV system and broadcasts it on the basis of the U.S.Pat.No.4613901 patent of GilhousenIt is the system and method of descrambling selectively by a regular member's descrambler.

[0005]And what introduced and embodied the smart card to the video code (Video Cipher) system which performs descrambling is U.S.Pat.No.5111504This the system of Gilhousen like "the information processor (Information Processor)" applicable to a descramblerand "a smart code (smart card)." It divides into "the protection element (Security Element)" for which it can substitute twoand embodies in it.
[0006]Thereforeif a scrambling system is embodied like drawing 1 with the application of said methoda descrambling system will be embodied like drawing 2.
[0007]Namelythe illegal viewing-and-listening arrester of the conventional digital video systemThe scramble of the television signal Vi is carried out according to general standard information (Common Category Key) CK and initialization vector (Initialization Vector) PKThe television signal SVo by which scramble was carried

outand the scrambler 101 which outputs scrambling information ($E_{U(D)}$ $E_{U(S)}$ (CK)E_{CK} (PK))The smart card 103 which enciphers the information (A (D)A (S)) for descrambling to descrambling information (U (S)) (Encryption)The information ($EA_{(D)}$ [$EA_{(S)}$ (WK)]) for descrambling of this smart card 103 is decoded (Decryption). It comprises the information processor 102 restored to the original television signal DVo by descrambling the transmission television signal SVo of said scrambler 101. A (D) is an attestation key (Authentication Key) of the information processor 102 hereA (S) is an attestation key of the smart card 103U (D) is the unit key (Unit Key) of said information processor 102and U (S) is an unit key of said smart card 103.

[0008]Under the present circumstancesthe 1st encryption machine 111 with which said scrambler 101 enciphers general key CK to the information (U (D) U (S)) for descramblingThe 2nd encryption machine 112 which enciphers initialization vector PK to general key CKIt comprises the 3rd encryption machine 113 which enciphers initialization vector PK to output E_{CK} (PK) of said 2nd encryption machine 112and the scrambling execution end 114 which carries out the scramble of the television signal Vi according to the output WK of said 3rd encryption machine 113.

[0009]Hereafterthe process of a device of operation is explained conventionally which was constituted in this way.

[0010]When it is going to transmit a television signal by Transmission Systems Divisionthe scrambler 101 general standard information (Common Category Key) CK with the 1st encryption machine 111 Firstthe information (U (D)) for descramblingEncipher to (U(S)) and initialization vector information (Initialization Vector) PK is enciphered to general standard information CK by the 2nd encryption 112Initialization vector information PK is enciphered to the output (E_{CK} (PK)) of said 2nd encryption machine 112 with the 3rd encryption machine 113and it outputs to the scrambling processing end 114. Under the present circumstancesthe scrambling processing end 114 carries out the scramble of the television signal Vi on the basis of the output WK of the 3rd code machine 113. Herethe scrambling information WK appears in $E_{ECK(PK)}$ (PK).

[0011]Encipherment information [as opposed to / by this / general standard information CK in the scrambler 101] ($E_{U(D)}$ $E_{U(S)}$ (CK))The encipherment information (E_{CK} (PK)) over initialization vector information PK and the television signal SVo by which scramble was carried out will be transmitted to the information processor 102.

[0012]When the television signal SVo by which scramble was carried out is descrambled on the other handAfter the smart card 103 enciphers the information WK required for descrambling to the certification information (A (D)) of the information processor 102and own certification information (A (S))The enciphered descrambling information ($E_{A(D)}$ [$E_{A(S)}$ (WK)]) is outputted to the information processor 102.

[0013]The information processor 102 decodes the enciphered information ($E_{A(D)}$ [$E_{A(S)}$ (WK)]) which was outputted from the smart card 103 by thisIt will restore to the original television signal DVo by descrambling the television signal SVo transmitted

from SUKUNRABURA 101 using this.
[0014]Hereit is for improving security nature from illegal viewing and listening and a copy to apply encryption (Encryption) to the information transmission between the information processor 102 and the smart card 103.
[0015]For examplethe items (spec.) of a GA (Grand Alliance) high-definition TV system support a CA systemand the function required for a transmission protocol is embodied. In the meaning of supporting all the usable descrambling methods and the key encryption (Key Encryption) methodsthe function embodied by this system is flexible (Flexible).
It is usefuland the scramble of the bit stream can be carried out selectivelyand the flexibility (Flexibility) which can apply CA function per element stream is secured. Herescrambling means the process changed in order to mean making a data bit stream into irregularity (Random) and to protect information data from the conversion-to-its-own-use person who enciphers (Encryption) based on information data. That isa CA system makes irregular the data transmitted using a scramblerWhile preventing from decoding to ** the decoder by the side of the conversion-to-its-own-use person who is going to view and listen to TV broadcast without noticeThe decoder of the users to whom TV broadcast was permitted enables it to decode in normal the TV broadcast signal received by providing the information which formats a descrambler circuit.
[0016]Being able to embody the transmission protocol of MPEG for said operation in a format like drawing 3such a transmission protocol has the two characteristics which support CA function.
[0017]It tells whether the scramble of the 1st2-bit Transport-scrambling-control filled **and the transmission stream was carried outand what kind of scrambling key when scramble was carried outwas used.
[0018]The enciphered scrambling information is stored in such FIRUDO by the function which inserts each data into GA Transmission Systems Division using Transport-private-date FIRUDO in the adaptation (Adaptation) header of the 2nd transmission stream.
[0019]the transmission protocol of MPEG like drawing 3 which has said characteristic -- a transmission header and a PES (Packetized Elementary Stream) header -- andalthough an audio and a video data are transmitted respectively or simultaneous succeedinglyA transmission header comprises a ring header (Link Header)an adaptation headerand a play load (playload) field.
[0020]Herelink header (Link header) has a length of 4 bytesand length with a variable adaptation header.
[0021]Transport-scrambling-control FIRUDO is inserted in said link headerIf the value of this FIRUDO is "00"they are Not-Scrambled and "10"they are the Even key and "11" and they are the Odd key and "01"it will be recognized to be Reserved.
[0022]And a flag bit and Transport-private-data FIRUDO are contained in an

adaptation headerand a 1-bit Transport-private-data flag is included in said flag bit. The PES header of the transmission protocol of MPEG like drawing 3 is constituted like drawing 4.

[0023]Although FIRUDO for digital storage DSM like digital VCR exists in this PES headerit is constituted including PES HEDDAFIRUDO which has a PES header flag field which has the length of 14 bits of such filled **and variable length.

[0024]In said PES header flag fieldit constitutes including 1 bit CR (Copyright) flag1 bit OC (original-or-copy) flag2 bits PD flag1 bit TM flagand 1-bit AC flag.

[0025]and PES header filled ** -- it has variable length and a partial area is set up by PD and TM which were contained to the PES header flag fieldand AC flag. Namelywith a PES header flag a PTS/DTS fieldIf the value of PD flag is "00"do not existbut if it is "10"40 bitsIf it is "11"will become 80 bitsand if the value of a DSM Trick Mode filled ** TM flag is "0"it does not existIt should be 8 bitswhen it will become 8 bits and an Additional Copy Info. filled ** AC flag will be set with "1"if it is "1."

[0026]Scrambling information was transmitted and by applying such a format showed the process descrambled using this information to drawing 5.

[0027]Herewith the key by which the descrambling system is used for the present descramblingthe key as which the next was enciphered should be decoded and the descrambler must store 2the "Odd key" and the "Even key." And the scrambling system must set and transmit the value of transport-scrambling-control FIRUDO in a link header with the method by which the present transmission stream is descrambled.

[0028]By thisa descrambler will descramble and decode received dataafter distinguishing the "Even or Odd" key with the value of Transport-scrambling-control FIRUDO of the transmission header decoded with received data.

[0029]With namelythe value of Transport-scranmbling-control FIRUDO which the data of a format like drawing 5 was transmitted and was decoded with the smart card. When the descrambler is descrambling the frame of eye K_{2n-1} watch by the Odd keyA smart card decodes Transport-scrambling-control FIRUDO with the frame of eye K_{2n} watch descrambled nextand such operation is performed one by one.

[0030]on the other handthe ATV decoder which performs CA function is embodied like drawing 6although things can be carried outSuch an ATV decoder 110 will build the descrambler which needs high speed operation in the transmission demultiplexer 105and a DES algorithmthe stream SAIPA (Stream Cipher) algorithm using PN sequenceetc. will perform descramblingThe key (Encrypted Key) enciphered by this ATV decoder 110 is decrypted with the smart card 103 (Decryption).

[0031]Herethe interface of the smart card 103 and the ATV decoder 110 is made by ISO-7816 standards etc.

[0032]That isafter the signal received with the tuner gets over by a recovery and the error correcting section 104the error generated at the time of transmission is corrected via RS decodingand working example of drawing 6 is inputted into the transmission demultiplexer 105 of the ATV decoder 110and is descrambled.

[0033]Under the present circumstancesthe microcontroller 109 calculates the control signal and data which were descrambledtransmits the encipherment information for descrambling to the smart card 103and said smart card 103 decodes the transmitted encipherment informationand it transmits it to the ATV decoder 110. Under the present circumstancesthe transmission JIMARUCHI plexor 105 will restore a compression video signala compression audio signala control signaland data based on descrambling information. Therebyafter the video decoder's 107 elongating and making a note of a compression audio signal and carrying out temporary storage to 106the storage data is outputtedan image is displayedand the audio decoder 108 elongates a compression audio signaland reproduces an audio. The microcontroller 109 deciphers the control signal and data which were outputted from the transmission JIMARUCHI plexor 105and controls operation of said video decoder 107 and the audio decoder 108.

[0034]On the other handa block SAIPA (Block-cipher) algorithm like DES and the stream SAIPA (Stream-cipher) algorithm using PN sequence are used general most widely in the various methods used for encryption. Howeversince even a cryptographic key performs encryption and decryption with a chiselkey management (Key Management) and key distribution (Key Distribution) are difficult for such a method.

[0035]Thereforea public key (Public-Key) cipher system like U.S.Pat.No.4200770 was proposed as solution to this. This method enciphers using the public key which is an exhibited keyand decodes by an own secret key (Secret key). And U.S.Pat.No.4405829 has improved such a public key encryption-ized methodembodied with the encryption systemand it is known as an RSA encryption algorithm.

[0036]

[Problem(s) to be Solved by the Invention]Howeversaid public key encryption-ized method has the demerit of being unsuitable in high-speed encryption. Although the CA system aimed at preventing illegal viewing and listeningto the program distributed via DSM like digital VCRthere was no method of protecting against an illegal copy.

[0037]Namelyalthough the protection to the program supplied by a recording medium like DSM means prevention of an illegal copyBeing hard to apply the copy prevention (Copy Protection) method applied to the existing analog VCR system to the storage of a digital systemthe research to the copy preventing system for DSM is not independently progressing until now.

[0038]Thereforeare for this invention solving this problemand the purposeThe bit stream by which scramble was carried outand the enciphered key which were used for scrambling are transmitted in a mutually different courseBy descrambling a bit stream and preventing from performing normal decoding only at a bit stream based on the informationafter decoding the enciphered key with a smart cardIt is in providing illegal viewing and listening and the copy prevention method of the digital video system which prevents illegal viewing and listening and a copy.

[0039]Such this invention makes a PPV (Pay Per View) function much more powerful including the function which introduces a smart card with a CA system and checks a fee automatically (checking)By adding various functions by substitution of a smart cardupgrade (Upgrade) of the system performance can be carried out easily.
[0040]Since this invention can carry out sharp reduction of the key daily dose of the data protected since transmission data is separated and attestation and a key exchange process are automatically performed at the time of connection between digital VCR for the time of power-onor recordingIt does not operate and the reliability of a protection feature is made to improve further in an illegal smart card.
[0041]
[Means for Solving the Problem]Illegal viewing and listening and a copy prevention method of a digital video system by this inventionA distinction stage which distinguishes whether scramble (scramble) of the data inputted was carried outIf distinguished from data by which scramble was carried out in said distinction stageafter dividing into a bit stream and a key stream said data by which scramble was carried outDecode a separated key streamdecipher key informationand descrambling (descramble) of said separated bit stream is carried out according to key informationIf distinguished from a regeneration stage displayed in a display deviceand data by which scramble was carried out in said distinction stageRecord on a recording medium by data status with which a bit stream and a key stream were mixed according to record or copying mode and by which scramble was carried outorA recording level which is mixed with a bit stream and recorded on a recording medium after dividing into a bit stream and a key stream data by which scramble was carried out and enciphering a separated key streamIf distinguished from data by which scramble was carried out in said distinction stageafter dividing into a bit stream and a key stream data by which scramble was carried outDecrypt a key stream separated according to "PPC" mode or "backup copy (Back-up Copy)" mode to key information by the side of recordand transmitorIt consists of a transmission stage of decrypting a separated key stream twice and transmitting it to own key information and key information by the side of recordand said regeneration stagea recording leveland a transmission stage can be performed simultaneous or selectivelyand the above-mentioned purpose is attained by that.
[0042]According to a certain embodimentif distinguished from data by which scramble is not carried out in said distinction stagedata by which scramble is not carried out will not apply illegal viewing and listening and a copy preventing function.
[0043]According to a certain embodimentsaid regeneration stage decrypts a separated key stream with a decryption algorithm to an MPEG bit streamand deciphers key information. In a certain embodimentcopying operation of said recording levelThe 1st step that enciphers a key stream to own key informationand the 2nd step that distinguishes whether a key stream enciphered in the 1st step is in "PPC" modeor it is in "backup copy" modeIf distinguished from "PPC" mode in said 2nd

stepafter enciphering to key information by the side of record of a key stream decrypted and transmitted to key information by the side of recordThe 3rd step that is inserted in a position corresponding to an index codeand is recorded like a bit streamIf distinguished from "backup copy" mode in said 2nd stepit will encipher to key information by the side of record of a key stream decrypted and transmitted to own key information and key information by the side of recordAfter decrypting to key information on the selfit inserts in a position corresponding to an index codeand is that it is ****** with the 4th step recorded like a bit stream.

[0044]In a certain embodimentsaid 3rd-step "PPC" mode operationThe 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after separating a bit stream and a key streamThe 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record after enciphering to own key informationA recording level which is mixed to a bit stream transmitted in said 1st transmission stageand is recorded on a recording medium after enciphering a key stream transmitted in said 2nd transmission stage to key information by the side of record corresponding to an index codeIf it reproduces by completing record according to said recording level in a certain embodiment which is that it is ******After dividing a reproduced bit stream (S_{KS}(BS)+E^G (KS)) into a bit stream (S_{KS} (BS)) and a key stream (E^G (KS))A separation stage which inserts the index code IDX in a portion from which a key stream (E^G (KS)) was separatedand an encryption stage which enciphers a key stream (E^G (KS)) separated in said separation stage to own key informationA decipherment stage which deciphers key information by decrypting a key stream enciphered in said encryption stage to own key information and an MPEG bit streamA decryption stage which descrambles said separated bit stream (S_{KS} (BS)) based on key information deciphered in said decipherment stage is included.

[0045]In a certain embodimentsaid 4th-step "backup copy" mode operationThe 1st transmission stage of inserting and transmitting an index code to a portion from which the key stream was separated after separating a bit stream and a key streamThe 2nd transmission stage of decrypting and transmitting a key stream separated in said 1st transmission stage to key information by the side of record of an enciphered key streamand own key information after enciphering to own key informationAfter enciphering a key stream transmitted in said 2nd transmission stage to key information by the side of record corresponding to an index codeit mixes to a bit stream transmitted in said 1st transmission stageand is that it is ****** with a recording level recorded on a recording medium.

[0046]If it reproduces by completing record according to said recording level in a certain embodimenta reproduced bit stream (S_{KS}(BS)+D^{SC}_{AK} [E^G (KS)])After separating a bit stream (S_{KS} (BS)) and a key stream (D^{SC}_{AK} [E^G (KS)])A separation stage which inserts the index code IDX in a portion from which a key stream (D^{SC}_{AK} [E^G (KS)]) was separatedIn an encryption stage which enciphers twice a key stream (D^{SC}_{AK} [E^G (KS)])

separated in said separation stage to own key informationand said encryption stageBy decrypting a key stream enciphered twice to own key information and an MPEG bit streamA decipherment stage which deciphers key informationand a decryption stage which descrambles a separated bit stream (S_{KS} (BS)) based on key information deciphered in said decipherment stage are included.

[0047]Illegal viewing and listening and a copy prevention method of a digital video system by this inventionIf data by which scramble was carried out is inputtedafter dividing into a bit stream and a key stream said data by which scramble was carried outDecode a separated key streamdecipher key informationand said separated bit stream is descrambled based on deciphered key informationBy a regeneration stage displayed in a display deviceand data status with which a bit stream and a key stream were mixed when data by which scramble was carried out was inputted and by which scramble was carried out. It consists of a recording level recorded on a recording mediumsaid regeneration stage and a recording level can be performed simultaneous or selectivelyand the above-mentioned purpose is attained by that.

[0048]According to a certain embodimentsaid regeneration stage decodes a separated key stream with a decryption algorithm to an MPEG bit streamdeciphers key informationis the deciphered key information and distinguishes a descrambling method.

[0049]If it reproduces by completing record according to said recording level in a certain embodimentafter dividing a reproduced bit stream (S_{KS}(BS)+E^G (KS)) into a bit stream (S_{KS} (BS)) and a key stream (E^G (KS))A separation stage which inserts the index code IDX in a portion from which a key stream (E^G (KS)) was separatedOwn key information is received in a key stream (E^G (KS)) separated in said separation stageBy decrypting a key stream enciphered twice to own key information and an MPEG bit stream in an encryption stage enciphered by an encryption algorithmand said encryption stageA decipherment stage which deciphers key informationand a decryption stage which descrambles said separated bit stream (S_{KS} (BS))and is displayed in a display device based on key information deciphered in said decipherment stage are included.

[0050]Illegal viewing and listening and a copy prevention method of a digital video system by this inventionIf a key stream enciphered to own key information at the time of a copy is transmittedA distinction stage which distinguishes whether it is in "backup copy" modeor it is in "PPC" modeThe 1st transmission stage of decrypting and transmitting said key stream to key information by the side of record if distinguished from the [PPC" mode in said distinction stageAfter enciphering to key information by the side of record of a key stream transmitted in said 1st transmission stagean enciphered key stream is inserted in a position corresponding to an index codeIf distinguished from "backup copy" mode in the 1st recording level recorded on a recording medium like a bit streamand said distinction stageThe 2nd transmission stage of decrypting a key stream twice and transmitting it to own key information and key information by the side of recordAfter enciphering a key stream transmitted in

said 2nd transmission stage to key information by the side of recordAn enciphered key stream is inserted in a position corresponding to an index codeit is that it is ****** with the 2nd recording level recorded on a recording medium like a bit streamand the above-mentioned purpose is attained by that.
[0051]According to a certain embodimentsaid 1st transmission stage is transmittedafter decrypting a key stream enciphered to the own key information Ak to the own key information Ak and decrypting to key information aluminum by the side of record further.
[0052]According to a certain embodimentsaid 2nd transmission stage is transmittedafter decrypting twice a key stream enciphered to the own key information Ak to the own key information Ak and decrypting it to key information aluminum by the side of record further.
[0053]Illegal viewing and listening and a copy prevention method of a digital video system by this inventionIf a key stream (E^{G} (KS)) is detected at the time of reproduction of a recording mediumit will distinguish from the "PPC" recording mediumAfter enciphering a key stream to own key informationdecode for own key information and key information is decipheredA "PPC" mode reproduction stage which descrambles a bit stream using key information and an index code which were decipheredIf a key stream (D^{SC}_{AK} [E^{G} (KS)]) decrypted to own key information at the time of reproduction of a recording medium is detectedAfter distinguishing from a "backup copy" recording medium and enciphering twice to key information by the side of self and recordIt decodes for own key informationkey information is decipheredit is that it is ****** with deciphered key information and a "backup copy" mode reproduction stage which descrambles a bit stream using an index codeand the above-mentioned purpose is attained by that.
[0054]Illegal viewing and listening and a copy arrester of a digital video system by this inventionA recovery and an error correction means which carry out the strange recovery of the analog broadcasting signaland carry out RS decodingAfter dividing into a bit stream and a key stream a record signal which transmits said recovery and an output of an error correction means to record/playback equipmentand is reproduced with its record/playback equipment and by which scramble was carried outA copy preventing process means to encipher a separated key streamand a decoder means to descramble a bit stream outputted from said recovery and an error correction meansor a copy preventing process means based on descrambling informationA key stream enciphered by said copy preventing process means is decodedit constitutes [**] with a smart means to output to said decoder means as descrambling informationand the above-mentioned purpose is attained by that.
[0055]In a certain embodimenta decoder means by which said recovery and an error correction means were connected is connected to a smart meansBy decoding a key stream of said decoder means for own key information with said smart cardand outputting descrambling information to said decoder meansit constitutes so that an

illegal viewing-and-listening preventing function may be performed.
[0056]According to a certain embodimenta copy preventing process means by which said recovery and an error correction means were connected records only after being connected to digital recording/playback equipment.
[0057]While connecting to a smart card a key stream line of a copy prevention means where said digital recording/playback equipment were connected in a certain embodimenta bit stream line is connected to a decoder meansIllegal reproduction is preventedwhen said copy preventing process means and a decoder means are connectedand said smart card decodes a key stream of said copy preventing process means corresponding to an index code of said decoder means for own key information and outputs to said decoder means.
[0058]According to a certain embodimentsaid copy preventing process means enciphers a key stream separated from regenerative data of digital recording/playback equipment at the time of recording-medium reproduction in "PPC" mode for own key informationand transmits it to a smart card.
[0059]According to a certain embodimentsaid copy preventing process means enciphers twice for own key informationand transmits a key stream separated from regenerative data of digital recording/playback equipment at the time of reproduction medium reproduction in "backup copy" mode to a smart card.
[0060]In a certain embodimentsaid copy preventing process meansIt is that it is ****** with RAM which memorizes key information peculiar to a smart cardan algorithm storage memory which stores an encryption algorithmand a processor which executes an enciphered program of said algorithm storage memory for key information on said RAM.
[0061]The 1st algorithm storage memory in which said smart card stores a decryption algorithm program for bit SUTORIMU in a certain embodimentIt constitutes [**] with the 2nd algorithm storage memory which stores an own decryption algorithm programROM which stores own key informationand RAM which carries out temporary storage of the key information on other smart cards.
[0062]Illegal viewing and listening and a copy arrester of a digital video system by this inventionA 1st copy preventing process means to encipher a separated key stream after dividing regenerative data of the 1st digital recording / playback equipment into a bit stream and a key streamThe 1st and 2nd smart card that decrypts a key stream enciphered by said 1st copy preventing process means to own key information and key information by the side of recordAfter enciphering a key stream of said 1st smart card transmitted via said 2nd smart card for own key informationwith a bit stream from which an enciphered key stream was separated. It outputs to the 2nd digital recording / playback equipmentand constitutes [**] with a 2nd copy preventing process means to record on a recording mediumand the above-mentioned purpose is attained by that.
[0063]According to a certain embodimentafter said 1st copy preventing process

means enciphers a key stream to the own key information Akit is transmitted to the 1st smart card.
[0064]According to a certain embodimentwhen it is [said 1st smart card] in "PPC" modeafter decrypting a key stream of the 1st copy preventing process means to own key information and key information by the side of recordit is transmitted to the 2nd smart card.
[0065]According to a certain embodimentsaid 2nd copy preventing process means mixes with a bit stream of the 1st copy preventing process means a key stream transmitted with the 2nd smart cardafter enciphering to own key information aluminum.
[0066]According to a certain embodimentwhen it is in "backup copy" modesaid 1st smart card decodes it to key information by the side of recordafter it decodes a key stream of the 1st copy preventing process means twice to own key information.
[0067]According to a certain embodimentsaid 2nd copy preventing process means enciphers a key stream transmitted from the 2nd smart card to own key informationand mixes the enciphered key stream with a bit stream.
[0068]In a certain embodimentsaid 1st and 2nd copy preventing process meansIt constitutes [**] with RAM which stores key information peculiar to a smart cardan algorithm storage memory which stores an encryption algorithmand a processor which executes an enciphered program of said algorithm storage memory using key information on said RAM.
[0069]In a certain embodimentsaid 1st and 2nd smart cardThe 1st algorithm storage memory which stores a decryption algorithm program for a bit streamIt constitutes [**] with the 2nd algorithm storage memory which stores an own decryption algorithm programROM which stores own key informationand RAM which carries out temporary storage of other smart key information.
[0070]
[Embodiment of the Invention]Hereafterthis invention is explained in detail with reference to an accompanying drawing.
[0071]This invention can be applied to all the record/playback equipment which can record and reproduce a digital signaland makes DVCR one working example in this invention for the facilities of explanation.
[0072]Thereforethe recovery and the error correcting section 1 which carry out the strange recovery of the broadcasting signal of an analogand carry out RS decoding as working example of this invention is shown in drawing 7The ATV decoder 2 which descrambles said recovery and the output of the error correcting section 1 based on descrambling informationThe copy preventing process part 4 which divides into a bit stream and a key stream the record signal by which scramble was carried outand enciphers the separated key streamIt constitutes from the smart card 3 which decodes the index code of the key stream separated and enciphered in this copy preventing process part 4and said ATV decoder 2and outputs the descrambling

information KS to said ATV decoder 2.
[0073]RAM17 in which said copy preventing process part 4 stores key information peculiar to a smart card as shown in drawing 8It constitutes from the algorithm stores dept. 18 which stores an encryption algorithmand the processor 16 which executes the enciphered program of said algorithm stores dept. 18 for the key information on said RAM17.
[0074]The 1st algorithm stores dept. 12 in which said smart card 3 stores the decryption algorithm for a bit stream as shown in drawing 9The 2nd algorithm stores dept. 13 which stores an own decryption algorithmROM14 which stores own key informationand RAM15 which carry out temporary storage of the key information on other smart cardsIt constitutes from the processor 11 which performs encryption or decryption to the key information stored in said ROM14 or RAM15 with the storage algorithm of said 1st and 2nd algorithm stores dept.s 12 and 13.
[0075]Under the present circumstanceswhen said processors 11 and 16 can be constituted from WAIYADO logic (Wired Logic)or can use a microprocessor and use a microprocessorthey will build in the encryption algorithm for a smart card by a program.
[0076]Hereafterthe operation and the operation effect of this invention which were constituted in this way are explained.
[0077]Although an MPEG bit stream is transmitted in drawing 11 (a) thru/or a format as shown in (c) by this inventionDrawing 11 (a) is a format by which scramble is not carried outdrawing 11 (b) is the format by which scramble was carried out to the bit streamand drawing 11 (c) is the format to which the scramble of the bit stream was carried out selectively.
[0078]In this inventionwhen scramble is carried out to an MPEG bit streamif protection (protection) is added with any gestaltena premise will be carried out.
[0079]Thereforewhen the stream data (S_{KS}(BS)+E^{G} (KS)) in which the scramble of drawing 11 (b) or the format as shown in (c) was carried out to the copy preventing process part 4 are inputtedIf it separates into drawing 11 (d) thru/or a bit stream (S_{KS}(BS)+IDX) as shown in (e)and a key stream (E^{G} KS) by splitter (Splitter) as shown in drawing 10and a recording mode is performedIt is enciphered further and said separated key stream (E^{G} (KS)) is transmitted to the smart card 3.
[0080]Heresince illegal viewing and listening and a copy preventing function are applied only to the portion by which scramble was carried out when the scramble of the bit stream is carried out selectively as shown in drawing 11 (c)a partial protection feature can be performed.
[0081]Firstas shown in drawing 11 (a)when the bit stream by which scramble is not carried out is transmittedEven if the bit stream to which it strange-restored and which was decoded by the recovery and the error correcting section 1 is inputted into the copy preventing process part 4data is not transmitted to the smart card 3A bit stream is decoded without the ATV decoder 2 into which the bit stream of said

recovery and the error correcting section 1 was inputted also transmitting data to said smart card 3. Thereforerestriction [what] is also lost to viewing and listening and a copy.

[0082]The video and the audio signal which are outputted here from the signal inputted into a recovery and the error correcting section 1 from a tuner and the ATV decoder 2 are an analog signal. The signal outputted from a tuner is a signal by which VSB abnormal conditions were carried out from GA bit stream. And a bit stream and a key stream are the digital signals for digital DVCR among input output signals. Under the present circumstancesif it recordsa bit stream will be recorded on digital VCR and this recorded bit stream will be reproduced with general digital VCR. That issince there is no data transmitted to the smart card 3 in order that there may be no key informationeven if it passes a splitteras the MPEG bit stream which does not require scrambling is inputted into the copy preventing process part 4 and it is shown in drawing 10When scrambling does not startany restriction cannot be found in viewing and listening and a copy.

[0083]Separate into a bit stream and a key stream and this invention is transmitted with a line differentrespectivelywhen performing recording or a copy preventing functionbut. The information about a copy prevention method is carried and transmitted to addition copy information (Additional Copy Info.) FIRUDO in a PES header.

[0084]Under the present circumstancessince it is in the state where the information about a key was removed even if it transmits the bit stream without the enciphered key by which scramble was carried out by a public channelwhen it flows into a conversion-to-its-own-use persondescrambling cannot be performed to **. And since it is enciphered further and the separated key is transmitteda bit stream cannot be descrambled when there is no decoding algorithm. Thereforealthough this invention uses arbitrary FIRUDO with an MPEG transmission protocol for starting illegal viewing and listening and the prevention from a copyas for the bit stream by which scramble was carried outa copy preventing function is applied.

[0085]Firstby the decoder 2if it changes "Transport-scrambling-control filled" into "Not Scrambled" modesince descrambling is not performedthe conversion-to-his-own-use person cannot operate said FIRUDO. Since it determines it that whether copy prevention being made to be carried out by "Transport-scrambling-control filled" and a copy are possible (free-copy) for such a copy prevention method whether it is made to becomeOnly by operating this FIRUDOthe conversion-to-his-own-use person cannot cancel a copy preventing function.

[0086]By nextthe way a conversion-to-his-own-use person corrects "addition copy information (Additional Copy Info.) filled" in a PES header. Since correction of this FIRUDO transforms a protective method and the protective method itself is not disassembledbig damage is not done to a copy preventing function.

[0087]The copy prevention method supported by this invention which has such a

featurePPV (Pay Per View) and the PPP (Pay Per Play) function which are CA functions are considered as the default (Default)and there are the "No Copy" methoda "PPC (Pay Per Copy)" methodand the "Back-up Copy" method.
[0088]On other videotapesthe "No Copy" method is a copy the method of keeping from the ability to do at all hereand the "PPC" methodReceive a fee for every copy once and the "Back-up Copy" methodIt is a method which can display in normal the videotape copied when digital VCR by the side of other copied the videotape played with digital VCR by the side of one only with digital VCR by the side of oneand cannot be displayed in digital VCR by the side of other.
[0089]Hereafterthe copy prevention method of this invention and the flow of the MPEG bit stream by it are explained with reference to drawing 19 thru/or drawing 22.
[0090]Drawing 19 and 20 are the signal flow graphs to operation of a copy preventing process part at the time of record or reproduction modeDrawing 21 is a signal flow graph to operation of the smart card corresponding to said copy preventing process partand drawing 22 is a signal flow graph to record or the key exchange at the time of reproduction motionand an attestation process.
[0091]Firstthe signal flow of drawing 19 is explained. The copy preventing process part 4 into which the bit stream was inputted checks the existence of key informationdistinguishes how of scramblingit has key informationand when scramble is carried outit distinguishes whether it is the first recording or it is copy recording (S101).
[0092]Namelyin the case of the data by which scramble was carried outit is searched whether it is transmitted by the stream of a S_{KS}(BS)+IDX gestalt by separation of a bit stream (S_{KS} (BS)) and a key stream (E^G (KS))If the stream of a S_{KS}(BS)+IDX gestalt is detectedand it will distinguish from copy recording and will not be detectedit distinguishes from the first recording (S102).
[0093]By thiswhen distinguished from recording at firstthe stream (S_{KS}(BS)+E^G (KS)) with which the bit stream and the key stream were mixed by VCR5 is recorded on a tape (S106)When distinguished from copy recordingwhile a key stream (E^G (KS)) transmits the separated bit stream (S_{KS}(BS)+IDX) to the copy preventing process part 8 by the side of recordThe key information Ak is received in said key stream (E^G (KS))After enciphering furthermore (S105)it will record on a tape by VCR9 by the side of record by transmitting the enciphered key stream (E^{SC}_{Ak} [E^G (KS)]) to the smart card 7 by the side of record via the smart card 3 (S106).
[0094]On the contrarydrawing 20 is a signal flow graph in the case of playing the tape which recorded by a signal flow like drawing 19. The copy preventing process part 4 will distinguish whether (S108) and a recording function are "Back-up Copy" by separating and distinguishing a key streamwhen the bit stream reproduced with VCR is inputted (S107) (S110).
[0095]Under the present circumstancessaid stage (S110) will be distinguished from a recording tape at firstif there is no key informationit distinguishes from a common

recording tape and the enciphered key stream (E^G (KS)) is detected. If the key stream (D^{SC}_{Ak} [E^G (KS)]) decoded to the own key information Ak is detectedIt distinguishes from the recording tape of a PPC functionand if the key stream (D^{SC}_{Al} [E^G (KS)]) decoded to key information aluminum of other smart cards is detectedit will distinguish from the recording tape of the "Back-up Copy" function. By thiswhen general ** is a tapethe copy preventing process part 4The bit stream (S_{KS}(BS)+IDX) from which the bit stream (BS) was separated in the key stream (E^G (KS)) in the case of the recording tape for copy prevention is transmitted to the decoder 2 (S109).
[0096]And when a Back-up Copy function is applied to the copy preventing process part 4 at the time of playback of the recording tape for copy preventionBy enciphering twice by encryption algorithm E^{SC}_{Ak} (-) to the own key information Aka key stream (D^{SC}_{Ak} [E^G (KS)])The enciphered key stream (E^{SC}_{Ak} [E^G (KS)]) is transmitted to the smart card 3 (S111S112S113)When the Back-up Copy function is not appliedKeast RIMUMU (E^G (KS)) by enciphering by an encryption algorithm (E^{SC}_{Ak} (-)) to the own key information AkThe enciphered key stream (E^{SC}_{Ak} [E^G (KS)]) is transmitted to the smart card 3 (S112S113).
[0097]When performing the above operations in the copy preventing process part 4the smart card 3 operates a signal flow like drawing 21. If this is explained in detailsaid smart card 3 will distinguish whether the index code IDX or a key stream (E^G (KS)) is inputted by the decoder 2 by performing broadcast or reproduction (S114S115).
[0098]Under the present circumstancesthe smart card 3 distinguished from broadcast viewing and listening of the PPV function when the key stream (E^G (KS)) which is not the index code IDX was inputtedSaid key stream (E^G (KS)) is decoded by decryption algorithm D^G (-) to the bit stream GA (S116)and the key information KS is made to input into the decoder 2 (S117). By thisthe decoder 2 deciphers the key information KS on the smart card 3and distinguishes a descrambling methodBy descrambling a bit stream (S_{KS} (BS)) and outputting as an analog video signal and an audio signal by the distinguished descrambling methodthe televiewer can view and listen to broadcast.
[0099]On the other handif it is distinguished that the index code IDX was inputted in said stage (S115)After the smart card 3 decodes the key stream (E^{SC}_{Ak} [E^G (KS)]) inputted in the copy preventing process part 4 with a decryption algorithm (D^{SC}_{Ak} (-)) to the key information Ak (S118)reproduction motion -- or recording operation is distinguished (S119).
[0100]Under the present circumstancesif distinguished from reproduction motion in said stage (S119)the smart card 3 will decode the decrypted key stream (E^G (KS)) with the decryption algorithm (D^G (-)) to the bit stream GA (S116)The key information KS is made to input into the decoder 2 (S117). The decoder 2 deciphers the key information KS on the smart card 3 by thisDistinguish a descrambling method and the bit stream (S_{KS} (BS)) separated in the copy preventing process part 4 by the distinguished descrambling method is descrambledBy outputting an analog video signal

and an audio signalthe televiewer can view and listen to the recording program of a tape.

[0101]And if distinguished from recording operation in said stage (S119)it will be distinguished whether the smart card 3 is the "Back-up Copy" function (S120). If it is the "Back-up Copy" functionthe key information Ak is received in a key stream (E^{G} (KS))The key stream (D^{SC}_{Ak} [E^{G} (KS)]) (to key information aluminum) which decrypted with the decryption algorithm (D^{SC}_{Ak} (-)) (S121)and was decrypted It will decrypt with a decryption algorithm (D^{SC}_{Ak} (-)) (S122).

[0102]Under the present circumstancesthe key stream (D^{SC}_{Al} {D^{SC}_{Ak} [E^{G} (KS)]}) decrypted with the smart card 3 is transmitted to the record side (S123)If inputted into the copy preventing process part 8 via the smart card 7 (S124)it will be enciphered by an encryption algorithm (E^{SC}_{Al} (-)). By thisIf the smart card 7 is mixed with the bit stream (S_{KS} (BS)) which made mix the enciphered key stream (D^{SC}_{Ak} [E^{G} (KS)]) in the position specified by the index code IDXand was outputted from the copy preventing process part 4 by the side of reproductionIt will record on a tape by VCR9.

[0103]On the other handif it is distinguished from recording operation in said stage (S119) and it is distinguished that the PPC function which is not the "Back-up Copy" function in said stage (S120) was appliedThe smart card 3 decrypts a key stream (E^{G} (KS)) with a decryption algorithm (D^{SC}_{Al} (-)) to key information aluminum (S122)The decrypted key stream (D^{SC}_{Al} [E^{G} (KS)]) will be transmitted to the record side (S123).

[0104]Under the present circumstancesthe copy preventing process part 8 by the side of the record which received the input of the key stream (D^{SC}_{Al} [E^{G} (KS)]) via the smart card 7After enciphering by encryption algorithm E^{SC}_{Al} (-)The enciphered key stream (E^{G} (KS)) will be made to mix in the position specified by the index code IDXand it will mix with the bit stream (S_{KS} (BS)) outputted from the copy preventing process part 4 by the side of reproduction.

[0105]Thereforethe bit stream (S_{KS}(BS)+E^{G} (KS)) outputted from the copy preventing process part 8 is recorded on a tape by VCR9.

[0106]As mentioned abovein this inventionall the smart cards have a common algorithm and a common key to the encryption algorithm (E^{G} (-)) to an MPEG bit streamand a decryption algorithm (D^{G} (-)).

[0107]And although the encryption algorithm (E^{SC}_{Al} (-)) to a smart card and a decryption algorithm (D^{SC}_{Ak} (-)) have an algorithm with all the common smart cardskey information changes with smart cards. That iseach smart card will contain the attestation key applicable to own recognition name ID.

[0108]In performing the above operationsthe processing-ized operation including the process in which the attestation process and key which can recognize a partner are exchanged is required between a copy preventing process partand between smart cards and smart cards. Under the present circumstancesthe method with various method of using a symmetrical key algorithm [like a DES algorithm] whose

attestation process ismethod of using a public key algorithm like RSAmethod of using FS(Fiat-Shamir) Schemeetc. is shown.

[0109]By this inventionwhile performing the attestation process in which a public key algorithm was usedthe example of the method of exchanging keys was shown in drawing 22but. Such a method is a basis of the premise that the key reception means 201 and the key transmission means 202 which are going to attest a public key (ne) are sharingand will be applied.

[0110]Under the present circumstancesthe key reception means 201 is the smart card 1 by the side of a copy preventing process part or recordand the key transmission means 202 is the own smart card k.

[0111]Hereafterworking example of this invention which operates by the above flows is described with reference to drawing 12 thru/or drawing 18.

[0112]Since the circuit operates as shown in drawing 12 when bit stream BS like drawing 11 (a) by which scramble is not carried out is transmitted in this inventionAnalog video and an audio signal are outputted more for the bit stream by which strange recovery and RS decoding were carried out by the recovery and the error correcting section 1 to being decoded by the decoder 2.

[0113]Under the present circumstancesbit stream BS which is outputted from a recovery and the error correcting section 1 in recordIt is recorded on a tape by VCR5 via the copy preventing process part 4andin playbackanalog video and an audio signal are outputted by inputting into the decoder 2 bit stream BS played by VCR5and decoding it via the copy preventing process part 4. That issince data is not outputted to the smart card 3 from the copy preventing process part 4viewing and listening and a copy are not affected.

[0114]And when drawing 11 (b) or the bit stream by which scramble was carried out as shown in (c) entersin drawing 13operation like drawing 18 is performed by applying CA function.

[0115]Firstwhen performing a PPV functionoperate by a signal flow like drawing 13but. If the key stream (E^G (KS)) enciphered as the bit stream (S_{KS} (BS)) by which scramble was carried out is transmittedA recovery and the error correcting section 1 will correct the error generated during transmission via RS decodingafter restoring to the modulated input signal.

[0116]Under the present circumstancesif the decoder 2 separates a key stream (E^G (KS)) among a recovery and the output (S_{KS}(BS)+E^G (KS)) of the error correcting section 1 and outputs to the smart card 3The smart card 3 decodes said enciphered key stream (E^G (KS))and outputs the key stream KS to said decoder 2 further. By thisafter the decoder 2 deciphers the key stream KS of the smart card 3 and distinguishes a descrambling methodit will decode a bit stream (S_{KS} (BS)) and will output an analog video signal and an audio signal.

[0117]Herethe processor 11 will decode the key stream (E^G (KS)) enciphered with the decryption algorithm (E^G (-))and the smart card 3 like drawing 9 will output the

decoded key stream KS to the decoder 2.
[0118]On the other handwhen recording first the bit stream by which scramble was carried outoperate by a signal flow like drawing 14but. After an error is corrected via a recovery and RS decoding by a recovery and the error correcting section 1the transmitted bit stream (S_{KS}(BS)+E^{G} (KS)) is inputted into VCR5 via the copy preventing process part 4and is recorded on a tape.
[0119]When playing the bit stream recorded in this wayand it is a PPP functionoperate by a signal flow like drawing 15but. If the bit stream (S_{KS}(BS)+E^{G} (KS)) reproduced by VCR5 is inputted into the copy preventing process part 4After the copy preventing process part 4 divides the reproduced bit stream (S_{KS}(BS)+E^{G} (KS)) into a bit stream (S_{KS} (BS)) and a key stream (E^{G} (KS))Said separated key stream (E^{G} (KS)) is further enciphered by an encryption algorithm (E^{SC}_{Ak} (−))It outputs to the smart card 3and said separated bit stream (S_{KS} (BS)) carries out load of the index code IDX to the portion from which the key stream (E^{G} (KS)) was taken outand outputs it to the decoder 2.
[0120]Under the present circumstancesthe smart card 3 which received the input of the index code IDX via the decoder 2The key stream (E^{SC}_{Ak} [EG (KS)]) as which the copy preventing process part 2 was enciphered is decoded with the decryption algorithm (D^{SC}_{Ak} (−)) for a smart cardThe key stream KS which is descrambling information is outputted to said decoder 2 (S117). After the decoder's 2 deciphering the key stream KS of the smart card 3 and distinguishing a descrambling method by thisBy decoding the bit stream (S_{KS} (BS)) inputted via the copy preventing process part 4an analog video signal and an audio signal will be outputted.
[0121]And when recording the data recorded by a signal flow like drawing 14 with different VCRperform a PPC function like the signal flow of drawing 16but. When the bit stream (S_{KS}(BS)+E^{G} (KS)) reproduced by VCR5 is inputted into the copy preventing process part 4the copy preventing process part 4A bit stream (S_{KS}(BS)+E^{G} (KS)) is divided into a bit stream (S_{KS} (BS)) and a key stream (E^{G} (KS)). Thenencipher said separated key stream further by an encryption algorithm (E^{SC}_{Ak} (−))and it outputs to the smart card 3The index code IDX will be added to the portion from which said separated bit stream (S_{KS} (BS)) and the key stream (E^{G} (KS)) were taken outand it will output to the copy preventing process part 8 by the side of record.
[0122]Under the present circumstancesafter the smart card 3 by the side of reproduction decodes the key stream (E^{SC}_{Ak} [E^{G} (KS)]) enciphered in the copy preventing process part 4 with a decryption algorithm (D^{SC}_{Al} (−)) to key information aluminum stored in RAMThe decoded key stream (D^{SC}_{Al} [E^{G} (KS)]) will be outputted to the smart card 7 by the side of record. By thisif the smart card 7 by the side of record outputs to the copy preventing process part 8 by the side of record in response to the input of the key stream (D^{SC}_{Al} [E^{G} (KS)]) of the smart card 3 by the side of reproductionAfter said copy preventing process part's 8 enciphering said key stream (D^{SC}_{Al} [E^{G} (KS)]) and restoring to the enciphered original key stream (E^{G}

(KS))By mixing to the bit stream (G_{KS} (BS)) outputted from the copy preventing process part 4 by the side of playbackand outputting to VCR5 by the index code IDXit will record on other tapes.

[0123]The data of the tape recorded in such operation can apply a PPP functionand can play it by a signal flow like drawing 15. When recording the data recorded by a signal flow like drawing 14 with other VCRa Back-upCopy function can be performed like the signal flow of drawing 17.

[0124]That isif the bit stream (S_{KS}(BS)+E^{G} (KS)) reproduced by VCR5 is inputted into the copy preventing process part 4After dividing the copy preventing process part 4 into a bit stream (S_{KS} (BS)) and a key stream (E^{G} (KS))Encipher said separated key stream further by an encryption algorithm (E^{SC}_{Ak} (-))and it outputs to the smart card 3Said separated bit stream (S_{KS} (BS)) will add the index code IDX to the portion from which the key stream (E^{G} (KS)) was taken outand will output it to the copy preventing process part 8 by the side of record.

[0125]Under the present circumstancesafter the smart card 3 by the side of reproduction decrypts twice the key stream (E^{SC}_{Ak} [E^{G} (KS)]) enciphered in the copy preventing process part 4 with a decryption algorithm (D^{SC}_{Ak} (-)) to the key Ak of the self stored in ROMIt decodes with a decryption algorithm (D^{SC}_{Al} (-)) to key information aluminum furthermore stored in RAMThe decoded key stream (D^{SC}_{Al} {D^{SC}_{Ak} [E^{G} (KS)]}) will be outputted to the smart card 7 by the side of record. By thisif the key stream (D^{SC}_{Al} {D^{SC}_{Ak} [E^{G} (KS)]}) of the smart card 3 by the side of reproduction is outputted to the copy preventing process part 8 by the side of record via the smart card 7 by the side of recordBy enciphering to key information aluminumthe copy preventing process part 8 restores said key stream (D^{SC}_{Al} {D^{SC}_{Ak} [E^{G} (KS)]}) to the original cryptographic key stream (D^{SC}_{Ak} [E^{G} (KS)]). And the restored cryptographic key stream (D^{SC}_{Ak} [E^{G} (KS)])By the index code IDXit will mix to the bit stream (G_{KS} (BS)) outputted from the copy preventing process part 4 by the side of playbackwill output to VCR9and will record on other tapes.

[0126]Herea fee is calculated by the improved smart card 3 or 7.

[0127]Although the data recorded by performing such a Back-up Copy function is renewable only with VCR which recorded the former tapewhen it is normal playbackit operates by a signal flow like drawing 18 (a).

[0128]That isif the bit stream (S_{KS}(BS)+D^{SC}_{Ak} [E^{G} (KS)]) reproduced by VCR5 is inputted into the copy preventing process part 4The copy preventing process part 4 is divided into a bit stream (S_{KS} (BS)) and a key stream (D^{SC}_{Ak} [E^{G} (KS)]). Thensaid separated key stream (D^{SC}_{Ak} [E^{G} (KS)]) is enciphered twice by an encryption algorithm (E^{SC}_{Ak} (-))It outputs to the smart card 3and said separated bit stream (S_{KS} (BS)) adds the index code IDX to the portion from which the key stream (D^{SC}_{Ak} [E^{G} (KS)]) was taken outand outputs it to it to the decoder 2.

[0129]In this case. Via the decoder 2. The smart code 3 which received the input of the index code IDX decodes the key stream (E^{SC}_{Ak} [E^{G} (KS)]) enciphered in the copy

preventing process part 2 with the decryption algorithm (D^{SC}_{Ak} (−)) for a smart cardThe key stream KS which is descrambling information is outputted to said decoder 2. After the decoder's 2 deciphering the key stream KS of the smart card 3 and distinguishing a descrambling method by thisBy decoding the bit stream (S_{KS} (BS)) inputted via the copy preventing process part 4an analog video signal and an audio signal will be outputted.

[0130]And in the abnormal playback played with other VCR which is not VCR recorded at firstit will operate by a signal flow like drawing 18 (b)and playback of a tape becomes impossible.

[0131]That isif a copy tape is played by VCR9 which performed the tape copysplitting processing of the data (S_{KS}(BS)+D^{SC}_{Ak} [E^{G} (KS)]) played in the copy preventing process part 8 will be carried outA bit stream (S_{KS}(BS)+IDX) is separated.

[0132]Under the present circumstancesafter the separated key stream (D^{SC}_{Ak} [E^{G} (KS)]) was enciphered to own key information aluminumFurthermoreit is enciphered to key information aluminum (E^{SC}_{Al} {E^{SC}_{Al} (D^{SC}_{Ak} [E^{G} (KS)])})and is transmitted to the smart card 7. And since the smart card 7 cannot decode a bit stream (E^{SC}_{Al} {E^{SC}_{Al} (D^{SC}_{Ak} [E^{G} (KS)])})the key information KS is not transmitted to the decoder 6. Therebysince the smart card 7 does not descramble a bit stream (S_{KS} (BS))playback of a copy tape is not performed.

[0133]On the other handit is as follows when the term used for this invention for the understanding of this invention is defined.

[0134]1) GA bit stream 2KS=[which is not carried out as for BS:scramble −− $K_0K_1K_2$and ... K_i and ... a K_n]:key stream −− heretotal 3BS=[of the key by which n was used for scrambling −− $BS_0BS_1BS_2$...$BS_i$and ... a BS_n]:bit stream −− hereUnit 4S_{KS} (BS) which carries out the scramble of the BS_i as one segment of BS : MPEG bit stream S_{KS}(BS) =[SK_0 by which scramble was carried out (BS_0)SK_1 (BS_1)...SK_i (BS_i)and ... algorithm E^{G} (KS) used for enciphering and decrypting a key by SK_n(BS_n)]5E&D(and) :GA −− =[E^{G} (K_0) and E^{G} (K_1). ...E^{G} (K_i)...E^{G}(K_n)]D^{G}(KS) = [D^{G} (K_0)D^{G} (K_1)...D^{G} (K_i)...D^{G} (K_n)] −− =KS6IDX:[01 and 2...i. ... n]:index stream 7Ak: −− attestation key 8E^{SC}_{A}(−) [&D^{SC}_{A}] (−): of a smart card (k) −− encryption and the decryption algorithm of the smart card which used the attestation key (A) of the smart card as the key.

[0135]

[Effect of the Invention]Since this invention performs attestation and a key exchange process automatically at the time of power-on or connection between digital VCR as explained aboveSince illegal viewing and listening to an illegal smart card and a copy preventing function can be performed automatically and illegal viewing and listening and prevention from a copy can be performed still more nearly selectivelyIf scrambling processing is performed into the portion which wishes protection of a programa fee can also be imposed as a requestperforming illegal viewing and listening and prevention from a copy automatically.

[0136]And since this invention transmits a bit stream and the key stream made to separate in a differing courseWhen the quantity of protected data can be decreasedand illegal viewing and listening and a copy preventing function can be performed efficiently and the prevention from illegal viewing and listening and an illegal copy preventing function are embodied to a smart cardA fee can be discriminatorily imposed to each function by distinguishing PPVPPPPPCand a Back-up Copy function.

[0137]This invention is applicable to the copyright-to-program protection in DSM like digital VCR by embodying the copy preventing function of the digital signal which can be applied to DSM application. Thereforeapplication of this invention will acquire the effect that the reliability over illegal viewing and listening and the prevention from a copy can be raised.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram of a general scrambler.

[Drawing 2]It is a block diagram of a general descrambler.

[Drawing 3]It is an illustration figure of a transmission format.

[Drawing 4]It is a detailed illustration figure of the PES header in drawing 3.

[Drawing 5]It is an illustration figure of the transmission format by key distribution.

[Drawing 6]It is a block diagram of the conventional ATV decoder.

[Drawing 7]They are illegal viewing and listening of this inventionand a block diagram of a copy arrester.

[Drawing 8]It is a detailed block diagram of the copy preventing process part in drawing 7.

[Drawing 9]It is a detailed block diagram of the smart card in drawing 7.

[Drawing 10]It is an illustration figure showing the splitting (splitting) of the bit stream in drawing 8.

[Drawing 11](a) - (f) is an illustration figure showing the format of each bit stream.

[Drawing 12]It is an illustration figure showing the connected state of this invention.

[Drawing 13]It is an illustration figure showing the connected state of this invention.

[Drawing 14]It is an illustration figure showing the connected state of this invention.

[Drawing 15]It is an illustration figure showing the connected state of this invention.

[Drawing 16]It is an illustration figure showing the connected state of this invention.

[Drawing 17]It is an illustration figure showing the connected state of this invention.

[Drawing 18]It is an illustration figure showing the connected state of this invention.

[Drawing 19]It is a signal flow graph for operation of this invention.

[Drawing 20]It is a signal flow graph for operation of this invention.

[Drawing 21]It is a signal flow graph for operation of this invention.

[Drawing 22]It is a signal flow graph for the key exchange by this inventionand an attestation process.

[Description of Notations]

1 and 104 A recovery and error correcting section

26 ATV decoder

3 Smart card

4 and 8 Copy preventing process part

11 and 16 Processor

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－242438

(43)公開日　平成８年(1996)９月17日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	Ｚ	
Ｇ１１Ｂ　20/10		7736－5Ｄ	Ｇ１１Ｂ　20/10	Ｈ	
Ｈ０４Ｌ　9/18		8842－5Ｊ	Ｈ０４Ｌ　9/00	６５１	

審査請求　未請求　請求項の数31　ＯＬ　（全 28 頁）

(21)出願番号　特願平7－308004

(22)出願日　平成７年(1995)11月27日

(31)優先権主張番号　１９９４－３１３６４

(32)優先日　1994年11月26日

(33)優先権主張国　韓国（ＫＲ）

(71)出願人　590001669
エルジー電子株式会社
大韓民国，ソウル特別市永登浦区汝矣島洞20

(72)発明者　朴　兌▲ズン▼
大韓民國，　ソウル市，　種路區，　崇仁洞，　20－118

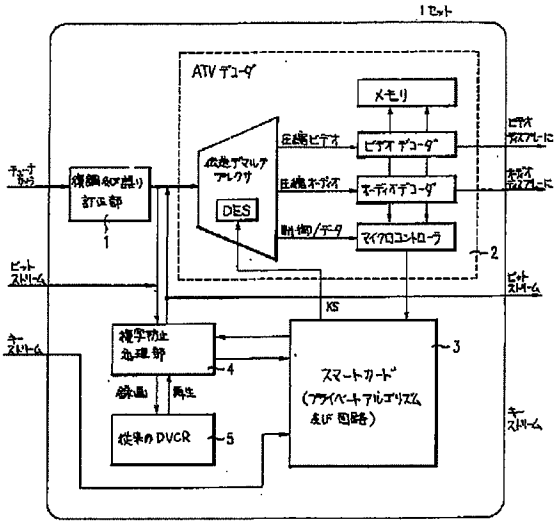
(74)代理人　弁理士　山本　秀策

(54)【発明の名称】　ディジタル映像システムの不法視聴／複写防止方法及び装置

(57)【要約】

【課題】　不法視聴及び複写を防止するディジタル映像システムの不法視聴及び複写防止方法を提供する。

【解決手段】　スクランブルされたビットストリームとスクランブリングに使用された暗号化されたキーを互いに異なる経路で伝送して、暗号化されたキーをスマートカードで復号した後、その情報に基づいてビットストリームをデスクランブルするようにし、ビットストリームのみでは正常的なデコードを行えないようにする



【特許請求の範囲】

【請求項１】　入力されるデータがスクランブル(scramble)されたかどうかを判別する判別段階と、
前記判別段階でスクランブルされたデータと判別されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、キー情報に応じて前記分離されたビットストリームをデスクランブル(descramble)して、ディスプレイ装置にディスプレイする再生段階と、
前記判別段階でスクランブルされたデータと判別されると、記録もしくは複写モードに応じて、ビットストリームとキーストリームが混合されたスクランブルされたデータ状態で記録媒体に記録したり、スクランブルされたデータをビットストリームとキーストリームに分離し、分離されたキーストリームを暗号化した後、ビットストリームと混合して記録媒体に記録する記録段階と、
前記判別段階でスクランブルされたデータと判別されると、スクランブルされたデータをビットストリームとキーストリームに分離した後、「ＰＰＣ」モードもしくは「バックアップ・コピー(Back-up Copy)」モードに応じて分離されたキーストリームを記録側のキー情報に対して復号化して伝送したり、分離されたキーストリームを自身のキー情報と記録側のキー情報に対して２回復号化して伝送する伝送段階とからなり、
前記再生段階、記録段階、伝送段階は、同時又は選択的に行うことができることを特徴とするディジタル映像システムの不法視聴及び複写防止方法。

【請求項２】　前記判別段階でスクランブルされていないデータと判別されると、スクランブルされていないデータは不法視聴及び複写防止機能を適用しないことを特徴とする請求項１記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項３】　前記再生段階は、分離されたキーストリームをＭＰＥＧビットストリームに対する復号化アルゴリズムで復号化して、キー情報を判読することを特徴とする請求項１記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項４】　前記記録段階の複写動作は、キーストリームを自身のキー情報に対して暗号化する第１段階と、第１段階で暗号化されたキーストリームが「ＰＰＣ」モードであるか、或いは「バックアップ・コピー」モードであるかを判別する第２段階と、
前記第２段階で「ＰＰＣ」モードと判別されると、記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第３段階と、
前記第２段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化し、その自身のキー情報に対して復号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第４段階とからなることを特徴とする請求項１記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項５】　前記第３段階の「ＰＰＣ」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第１伝送段階と、
前記第１伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、記録側のキー情報に対して復号化して伝送する第２伝送段階と、
前記第２伝送段階で伝送されたキーストリームをインデックスコードに対応して記録側のキー情報に対して暗号化した後、前記第１伝送段階で伝送されたビットストリームに混合して記録媒体に記録する記録段階とからなることを特徴とする請求項４記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項６】　前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+E^{G}(KS)$)をビットストリーム($S_{KS}(BS)$)とキーストリーム($E^{G}(KS)$)に分離した後、キーストリーム($E^{G}(KS)$)が分離された部分にインデックスコードＩＤＸを挿入する分離段階と、
前記分離段階で分離されたキーストリーム($E^{G}(KS)$)を自身のキー情報に対して暗号化する暗号化段階と、
前記暗号化段階で暗号化されたキーストリームを自身のキー情報とＭＰＥＧビットストリームに対して復号化することによりキー情報を判読する判読段階と、
前記判読段階で判読されたキー情報に基づいて前記分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルする復号化段階とを含むことを特徴とする請求項５記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項７】　前記第４段階の「バックアップ・コピー」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第１伝送段階と、
前記第１伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、暗号化されたキーストリームを記録側のキー情報と自身のキー情報に対して復号化して伝送する第２伝送段階と、
前記第２伝送段階で伝送されたキーストリームをインデックスコードに対応して、記録側のキー情報に対して暗号化した後、前記第１伝送段階で伝送されたビットストリームに混合して、記録媒体に記録する記録段階とからなることを特徴とする請求項４記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項８】　前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+D^{SC}{}_{AK}[E$

$^{G}(KS)]$)を、ビットストリーム($S_{KS}(BS)$)とキーストリーム($^{DSC}_{AK}[E^{G}(KS)]$)を分離した後、キーストリーム($^{DSC}_{AK}[E^{G}(KS)]$)が分離された部分に、インデックスコードＩＤＸを挿入する分離段階と、

前記分離段階で分離されたキーストリーム($^{DSC}_{AK}[E^{G}(KS)]$)を自身のキー情報に対して暗号化する暗号化段階と、

前記暗号化段階において、２回暗号化されたキーストリームを自身のキー情報とＭＰＥＧビットストリームに対して復号化することにより、キー情報を判読する判読段階と、

前記判読段階で判読されたキー情報に基づいて、分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルする復号化段階とを含むことを特徴とする請求項７記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項９】　スクランブルされたデータが入力されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、判読されたキー情報に基づいて、前記分離されたビットストリームをデスクランブルして、ディスプレイ装置にディスプレイする再生段階と、

スクランブルされたデータが入力されると、ビットストリームとキーストリームが混合されたスクランブルされたデータ状態で、記録媒体に記録する記録段階とからなり、

前記再生段階、記録段階は、同時若しくは選択的に行うことができることを特徴とするディジタル映像システムの不法視聴及び複写防止方法。

【請求項１０】　前記再生段階は、分離されたキーストリームを、ＭＰＥＧビットストリームに対する復号化アルゴリズムで復号してキー情報を判読し、判読されたキー情報で、デスクランブル方式を判別することを特徴とする請求項９記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項１１】　前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+E^{G}(KS)$)をビットストリーム($S_{KS}(BS)$)とキーストリーム($E^{G}(KS)$)に分離した後、キーストリーム($E^{G}(KS)$)が分離された部分に、インデックスコードＩＤＸを挿入する分離段階と、

前記分離段階で分離されたキーストリーム($E^{G}(KS)$)を自身のキー情報に対して、暗号化アルゴリズムで暗号化する暗号化段階と、

前記暗号化段階で２回暗号化されたキーストリームを、自身のキー情報とＭＰＥＧビットストリームに対して復号化することにより、キー情報を判読する判読段階と、

前記判読段階で判読されたキー情報に基づいて、前記分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルして、ディスプレイ装置にディスプレイする復号化段階と、を含むことを特徴とする請求項９記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項１２】　複写時に自身のキー情報に対して暗号化されたキーストリームが伝送されると、「バックアップ・コピー」モードであるか、もしくは「ＰＰＣ」モードであるかを判別する判別段階と、

前記判別段階で［ＰＰＣ」モードと判別されると、記録側のキー情報に対して前記キーストリームを復号化して伝送する第１伝送段階と、

前記第１伝送段階で伝送されたキーストリームを記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入して、ビットストリームのように記録媒体に記録する第１記録段階と、

前記判別段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して、キーストリームを２回復号化して伝送する第２伝送段階と、

前記第２伝送段階で伝送されたキーストリームを、記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入してビットストリームのように記録媒体に記録する第２記録段階と、からなることを特徴とするディジタル映像システムの不法視聴及び複写防止方法。

【請求項１３】　前記第１伝送段階は、自身のキー情報Ａｋに対して暗号化されたキーストリームを自身のキー情報Ａｋに対して復号化し、さらに記録側のキー情報ＡＩに対して復号化した後、伝送することを特徴とする請求項１２記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項１４】　前記第２伝送段階は、自身のキー情報Ａｋに対して暗号化されたキーストリームを、自身のキー情報Ａｋに対して２回復号化し、さらに記録側のキー情報ＡＩに対して復号化した後伝送することを特徴とする請求項１２記載のディジタル映像システムの不法視聴及び複写防止方法。

【請求項１５】　記録媒体の再生時にキーストリーム($E^{G}(KS)$)が検出されると「ＰＰＣ」記録媒体と判別して、キーストリームを自身のキー情報に対して暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いて、ビットストリームをデスクランブルする「ＰＰＣ」モード再生段階と、

記録媒体の再生時に自身のキー情報に対して復号化されたキーストリーム($^{DSC}_{AK}[E^{G}(KS)]$)が検出されると、

「バックアップ・コピー」記録媒体と判別して、自身と記録側のキー情報に対して２回暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いてビットストリームをデスクランブルする「バックアップ・コピー」モード再生

段階とからなることを特徴とするディジタル映像システムの不法視聴及び複写防止方法。

【請求項１６】　アナログ放送信号を変復調してＲＳデコードする復調及び誤り訂正手段と、
前記復調及び誤り訂正手段の出力を記録／再生装置に伝送し、その記録／再生装置で再生されるスクランブルされた記録信号をビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する複写防止処理手段と、
前記復調及び誤り訂正手段若しくは複写防止処理手段から出力されるビットストリームをデスクランブリング情報に基づいてデスクランブルするデコーダ手段と、
前記複写防止処理手段で暗号化されたキーストリームを復号して、前記デコーダ手段へデスクランブリング情報として出力するスマート手段とから構成したことを特徴とするディジタル映像システムの不法視聴及び複写防止装置。

【請求項１７】　前記復調及び誤り訂正手段が接続されたデコーダ手段をスマート手段に接続して、前記スマートカードで前記デコーダ手段のキーストリームを自身のキー情報で復号して、デスクランブリング情報を前記デコーダ手段へ出力することにより、不法視聴防止機能を行うように構成したことを特徴とする請求項１６記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項１８】　前記復調及び誤り訂正手段が接続された複写防止処理手段を、ディジタル記録／再生装置に接続して初めて録画を行うことを特徴とする請求項１６記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項１９】　前記ディジタル記録／再生装置が接続された複写防止手段のキーストリームラインを、スマートカードに接続するとともに、ビットストリームラインをデコーダ手段に接続し、前記複写防止処理手段とデコーダ手段を接続して、前記スマートカードが前記デコーダ手段のインデックスコードに対応する前記複写防止処理手段のキーストリームを自身のキー情報で復号して前記デコーダ手段へ出力することにより不法再生を防止することを特徴とする請求項１６記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２０】　前記複写防止処理手段は「ＰＰＣ」モードの記録媒体再生時にディジタル記録／再生装置の再生データから分離したキーストリームを自身のキー情報で暗号化してスマートカードへ伝送することを特徴とする請求項１９記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２１】　前記複写防止処理手段は、「バックアップ・コピー」モードの再生媒体再生時にディジタル記録／再生装置の再生データから分離したキーストリームを、自身のキー情報で２回暗号化してスマートカードへ伝送すること、を特徴とする請求項１９記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２２】　前記複写防止処理手段は、
スマートカード固有のキー情報を記憶するＲＡＭと、
暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、
前記ＲＡＭのキー情報で前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサとからなることを特徴とする請求項１６、１８、又は請求項１９のいずれかに記載するディジタル映像システム及び複写防止装置。

【請求項２３】　前記スマートカードは、
ビットストリムの為の復号化アルゴリズムプログラムを貯蔵する第１アルゴリズム貯蔵メモリと、
自身の復号化アルゴリズムプログラムを貯蔵する第２アルゴリズム貯蔵メモリと、
自身のキー情報を貯蔵するＲＯＭと、
他のスマートカードのキー情報を一時貯蔵するＲＡＭとから構成したことを特徴とする請求項１６、１７、又は請求項１９のいずれかに記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２４】　第１ディジタル記録／再生装置の再生データをビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する第１複写防止処理手段と、
前記第１複写防止処理手段で暗号化されたキーストリームを自身のキー情報と記録側のキー情報に対して復号化する第１、第２スマートカードと、
前記第２スマートカードを介して伝送された前記第１スマートカードのキーストリームを自身のキー情報で暗号化した後、暗号化されたキーストリームを分離されたビットストリームとともに、第２ディジタル記録／再生装置へ出力して、記録媒体に記録する第２複写防止処理手段と、から構成したことを特徴とするディジタル映像システムの不法視聴及び複写防止装置。

【請求項２５】　前記第１複写防止処理手段は、キーストリームを自身のキー情報Ａｋに対して暗号化した後、第１スマートカードへ伝送することを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２６】　前記第１スマートカードは、「ＰＰＣ」モードである時、第１複写防止処理手段のキーストリームを自身のキー情報と記録側のキー情報に対して復号化した後、第２スマートカードへ伝送することを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２７】　前記第２複写防止処理手段は、第２スマートカードで伝送されるキーストリームを自身のキー情報ＡＩに対して暗号化した後、第１複写防止処理手段のビットストリームと混合することを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写

防止装置。

【請求項２８】　前記第１スマートカードは「バックアップ・コピー」モードであるとき、第１複写防止処理手段のキーストリームを自身のキー情報に対して２回復号した後、記録側のキー情報に対して復号することを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項２９】　前記第２複写防止処理手段は、第２スマートカードから伝送されるキーストリームを自身のキー情報に対して暗号化し、その暗号化されたキーストリームをビットストリームと混合することを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項３０】　前記第１、第２複写防止処理手段は、スマートカード固有のキー情報を貯蔵するＲＡＭと、
暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、
前記ＲＡＭのキー情報によって、前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサと、から構成したことを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写防止装置。

【請求項３１】　前記第１、第２スマートカードは、ビットストリームのための復号化アルゴリズムプログラムを貯蔵する第１アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第２アルゴリズム貯蔵メモリと、
自身のキー情報を貯蔵するＲＯＭと、
他のスマートキー情報を一時貯蔵するＲＡＭとから構成したことを特徴とする請求項２４記載のディジタル映像システムの不法視聴及び複写防止装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はディジタル映像システムの不法視聴及び複写防止技術に関する。特にスマートカードを導入して分離されたキーストリームを復号してデスクランブリング方式を設定するようにすることにより、無断使用者の不法視聴及び複写を防止するディジタル映像システムの不法視聴／複写防止方法及び装置に関する。

【０００２】

【従来の技術】一般的なディジタル映像システムで不法視聴防止のためにConditional Access（以下、ＣＡという）システムの具現に関心が集中している。

【０００３】このようなＣＡシステムは、ケーブルＴＶや衛星放送などの有料チャンネルで放送信号をスクランブルされた形態で放送することにより、正式で金を払った使用者だけがデスクランブリングを介して碌に放送プログラムを視聴し得るようにするものである。たとえば、衛星放送受信機若しくは米国のＡＴＶ規格のGrandAllinace（以下、ＧＡという）システムは、ＣＡを支援するための機能を持っており、ＧＩ社のビデオ暗号(Video Cipher)のような衛星放送に使用されるスクランブリング／デスクランブリング装置も既に常用化された。

【０００４】一般的なＣＡシステムのためのスクランブリングシステムは、ＧＩ社のビデオ暗号(Video Cipher)システムであり、GilhousenのU.S.Pat.No.4613901特許を基礎とし、これは有料ＴＶシステムで正規加入者のデスクランブラへ伝送されるＴＶ信号をスクランブルして放送すると、正規加入者のデスクランブラで選択的にデスクランブルするシステム及び方法である。

【０００５】そして、デスクランブリングを行うビデオ暗号(Video Cipher)システムにスマートカードを導入して具現したものがU.S.Pat.No.5111504であり、これはGilhousenのシステムをデスクランブラに該当する「情報プロセッサー(Information Processor)」と「スマートコード(smart card)」のように代替可能な「保護エレメント(Security Element)」に２分割して具現したものである。

【０００６】従って、前記方式を適用してスクランブリングシステムを図１のように具現すると、デスクランブリングシステムは図２のように具現される。

【０００７】即ち、従来のディジタル映像システムの不法視聴防止装置は、一般規格情報(Common Category Key)ＣＫ及び初期化ベクトル(Initialization Vector)ＰＫに応じてＴＶ信号Ｖｉをスクランブルして、スクランブルされたＴＶ信号ＳＶoとスクランブリング情報($E_{U(D)}E_{U(S)}(CK)$、$E_{CK}(PK)$)を出力するスクランブラ１０１と、デスクランブリングのための情報(A(D)、A(S))をデスクランブリング情報(U(S))に対して暗号化(Encryption)するスマートカード１０３と、このスマートカード１０３のデスクランブリングのための情報($EA_{(D)}[EA_{(S)}(WK)]$)を復号(Decryption)して前記スクランブラ１０１の伝送ＴＶ信号ＳＶoをデスクランブルすることにより元のＴＶ信号ＤＶoに復元する情報プロセッサ１０２とから構成される。　ここで、A(D)は情報プロセッサ１０２の認証キー(Authentication Key)であり、A(S)はスマートカード１０３の認証キーであり、U(D)は前記情報プロセッサ１０２のユニットキー(Unit Key)であり、U(S)は前記スマートカード１０３のユニットキーである。

【０００８】この際、前記スクランブラ１０１は一般キーＣＫをデスクランブリングのための情報(U(D)U(S))に対して暗号化する第１暗号化器１１１と、初期化ベクトルＰＫを一般キーＣＫに対して暗号化する第２暗号化器１１２と、初期化ベクトルＰＫを前記第２暗号化器１１２の出力$E_{CK}(PK)$に対して暗号化する第３暗号化器１１３と、ＴＶ信号Ｖｉを前記第３暗号化器１１３の出力WKに応じてスクランブルするスクランブリング遂行端１１４とから構成される。

【０００９】以下、このように構成された従来装置の動作過程を説明する。

【００１０】まず、伝送システムでＴＶ信号を伝送しようとする場合、スクランブラ１０１は第１暗号化器１１１で一般規格情報(Common Category Key)ＣＫをデスクランブリングのための情報(U(D))、(U(S))に対して暗号化し、第２暗号化１１２で初期化ベクトル情報(Initialization Vector)ＰＫを一般規格情報ＣＫに対して暗号化し、第３暗号化器１１３で初期化ベクトル情報ＰＫを前記第２暗号化器１１２の出力($E_{CK}(PK)$)に対して暗号化してスクランブリング処理端１１４へ出力する。この際、スクランブリング処理端１１４は第３暗号器１１３の出力ＷＫを基準としてＴＶ信号Ｖｉをスクランブルする。ここで、スクランブリング情報ＷＫは$E_{ECK(PK)}(PK)$で表れる。

【００１１】これにより、スクランブラ１０１は一般規格情報ＣＫに対する暗号化情報($E_{U(D)}E_{U(S)}(CK)$)、初期化ベクトル情報ＰＫに対する暗号化情報($E_{CK}(PK)$)及びスクランブルされたＴＶ信号ＳＶoを情報プロセッサ１０２へ伝送することになる。

【００１２】一方、スクランブルされたＴＶ信号ＳＶoをデスクランブルする場合、スマートカード１０３は情報プロセッサ１０２の認証情報(A(D))と自身の認証情報(A(S))に対してデスクランブリングに必要な情報ＷＫを暗号化した後、その暗号化されたデスクランブリング情報($E_{A(D)}[E_{A(S)}(WK)]$)を情報プロセッサ１０２へ出力する。

【００１３】これにより、情報プロセッサ１０２はスマートカード１０３から出力された暗号化された情報($E_{A(D)}[E_{A(S)}(WK)]$)を復号し、これを用いてスクンラブラ１０１から伝送されたＴＶ信号ＳＶoをデスクランブルすることによって元のＴＶ信号ＤＶoに復元することになる。

【００１４】ここで、情報プロセッサ１０２とスマートカード１０３間の情報伝送に暗号化(Encryption)を適用することは、不法視聴及び複写から保安性を高めるためのものである。

【００１５】例えば、ＧＡ(Grand Alliance)高画質ＴＶシステムの内訳(spec.)はＣＡシステムを支援し、且つ伝送プロトコルに必要な機能が具現されている。このシステムに具現された機能は、使用可能な全てのデスクランブリング方法及びキー暗号化(Key Encryption)方法を支援するという意味において、フレキシブル(Flexible)であり、有用であり、且つビットストリームを選択的にスクランブルすることができて、エレメントストリーム単位でＣＡ機能を適用し得る融通性(Flexibility)が保障される。ここで、スクランブリングは、情報データに基づいて、データビットストリームを不規則(Random)にすることを意味し、暗号化(Encryption)する不法使用者から情報データを保護するために変換する過程を意味する。つまり、ＣＡシステムは伝送されるデータをスクランブラを用いて不規則にして、ＴＶ放送を無断で視聴しようとする不法使用者側のデコーダは碌にデコードできないようにする一方、ＴＶ放送が許可された使用者側のデコーダはデスクランブラ回路をフォーマットする情報を提供して受信されたＴＶ放送信号を正常的にデコードし得るようにするものである。

【００１６】前記動作のためのＭＰＥＧの伝送プロトコルは、図３のようなフォーマットで具現することができ、このような伝送プロトコルはＣＡ機能を支援する２つの特性がある。

【００１７】第１、２ビットのTransport-scrambling-controlフィールドは、伝送ストリームがスクランブルされたかどうかと、スクランブルされた場合にどんなスクランブリングキーが使用されたかを知らせてくれる。

【００１８】第２、伝送ストリームの適応(Adaptation)ヘッダ内のTransport-private-dateフィールドを用いて個々のデータをＧＡ伝送システム内に挿入する機能で、このようなフィールドには暗号化されたスクランブリング情報を貯蔵する。

【００１９】前記特性を有する図３のようなＭＰＥＧの伝送プロトコルは、伝送ヘッダ、ＰＥＳ(Packetized Elementary Stream)ヘッダ、そして引き続きオーディオ及びビデオデータをそれぞれ若しくは同時に伝送するが、伝送ヘッダはリングヘッダ(Link Header)、適応ヘッダ、及びプレイロード(playload)領域から構成される。

【００２０】ここで、リンクヘッダ (Link header)は４バイトの長さ、適応ヘッダは可変的な長さを有する。

【００２１】前記リンクヘッダには、Transport-scrambling-controlフィールドが挿入され、このフィールドの値は「００」であればNot-Scrambled、「１０」であればEvenキー、「１１」であれば、Oddキー、「０１」であれば、Reservedと認識することになる。

【００２２】そして、適応ヘッダにはフラグビットとTransport-private-dataフィールドが含まれ、前記フラグビット中には１ビットのTransport-private-dataフラグを含む。尚、図３のようなＭＰＥＧの伝送プロトコルのＰＥＳヘッダは図４のように構成される。

【００２３】このＰＥＳヘッダにはディジタルＶＣＲのようなディジタル記憶媒体ＤＳＭのためのフィールドが存在するが、このようなフィールドは１４ビットの長さを有するＰＥＳヘッダフラグ領域と可変長さを有するＰＥＳヘッダフィールドを含んで構成される。

【００２４】前記ＰＥＳヘッダフラグ領域には１ビットのＣＲ(Copyright)フラグ、１ビットのＯＣ(original-or-copy)フラグ、２ビットのＰＤフラグ、１ビットのＴＭフラグ、そして１ビットのＡＣフラグを含んで構成する。

【００２５】そして、ＰＥＳヘッダフィールドは可変的な長さを有し、ＰＥＳヘッダフラグ領域に含まれたＰＤ、ＴＭ、ＡＣフラグによって一部領域が設定される。即ち、ＰＥＳヘッダフラグでＰＴＳ／ＤＴＳ領域は、ＰＤ

フラグの値が「００」であれば存在せず、「１０」であれば４０ビット、「１１」であれば８０ビットとなり、ＤＳＭ Trick Modeフィールドは ＴＭフラグの値が「０」であれば存在せず、「１」であれば８ビットとなり、Additional Copy Info.フィールドはＡＣフラグが「１」とセットされるとき、８ビットとなっているべきである。

【００２６】このようなフォーマットを適用することにより、スクランブリング情報を伝送し、この情報を用いてデスクランブルする過程を図５に示した。

【００２７】ここで、デスクランブリングシステムは、現在デスクランブリングに使用されているキーとともに、次の暗号化されたキーが復号されているべきであって、デスクランブラは「Oddキー」と「Evenキー」のふたつを貯蔵していなければならない。そして、スクランブリングシステムは、現在の伝送ストリームがデスクランブルされる方式によって、リンクヘッダ内のtransport-scrambling-controlフィールドの値をセットして伝送しなければならない。

【００２８】これにより、デスクランブラは受信データで復号された伝送ヘッダのTransport-scrambling-controlフィールドの値によって「Even or Odd」キーを判別した後、受信データをデスクランブルして復号することになる。

【００２９】即ち、図５のようなフォーマットのデータが伝送されて、スマートカードで復号されたTransport-scranmbling-controlフィールドの値によって、デスクランブラがK_{2n-1}番目のフレームをOddキーでデスクランブルしているとき、スマートカードは次にデスクランブルするK_{2n}番目のフレームでTransport-scrambling-controlフィールドを復号し、このような動作は順次行われる。

【００３０】一方、ＣＡ機能を行うＡＴＶデコーダを例えば図６のように具現することできるが、このようなＡＴＶデコーダ１１０は伝送デマルチプレクサ１０５に高速演算が必要なデスクランブラを内蔵してＤＥＳアルゴリズムやＰＮシーケンスを用いたストリームサイパー(Stream Cipher)アルゴリズム等でデスクランブリングを行うことになり、このＡＴＶデコーダ１１０で暗号化されたキー(Encrypted Key)はスマートカード１０３で復号化(Decryption)される。

【００３１】ここで、スマートカード１０３とＡＴＶデコーダ１１０のインタフェースはISO-7816標準規格等によってなされる。

【００３２】即ち、図６の実施例はチューナで受信された信号が復調及び誤り訂正部１０４で復調された後、伝送時に発生された誤りがＲＳデコーディングを介して訂正され、ＡＴＶデコーダ１１０の伝送デマルチプレクサ１０５に入力されてデスクランブルされる。

【００３３】この際、マイクロコントローラ１０９はデスクランブルされた制御信号及びデータを演算して、スマートカード１０３にデスクランブリングのための暗号化情報を伝送し、前記スマートカード１０３は伝送された暗号化情報を復号してＡＴＶデコーダ１１０に伝送する。この際、伝送ジマルチプレクサ１０５がデスクランブリング情報に基づいて圧縮ビデオ信号、圧縮オーディオ信号、制御信号、及びデータを復元することになる。これにより、ビデオデコーダ１０７は圧縮オーディオ信号を伸張してメモリ１０６に一時貯蔵した後、その貯蔵データを出力して映像を表示し、オーディオデコーダ１０８は、圧縮オーディオ信号を伸張してオーディオを再生する。尚、マイクロコントローラ１０９は伝送ジマルチプレクサ１０５から出力された制御信号及びデータを判読して、前記ビデオデコーダ１０７及びオーディオデコーダ１０８の動作を制御する。

【００３４】一方、暗号化に使用されるいろんな方式の中で、ＤＥＳのようなブロックーサイパー(Block-cipher)アルゴリズム及びＰＮシーケンスを用いたストリームサイパー(Stream-cipher)アルゴリズムが一般的に一番広く使用されている。しかし、このような方式は暗号キー一つのみで暗号化及び復号化を行うので、キー管理(Key Management)及びキー分配(Key Distribution)が難しい。

【００３５】従って、これに対する解決策として、U.S. Pat. No. 4200770のようなパブリックキー(Public-Key)暗号化方式が提案された。この方式は公開されたキーであるパブリックキーを用いて暗号化を行い、自身のみの秘密キー(Secret key)で復号を行うものである。そして、このようなパブリックキー暗号化方式を改善して暗号化システムで具現したのがU.S. Pat. No. 4405829であり、ＲＳＡ暗号化アルゴリズムとして知られている。

【００３６】

【発明が解決しようとする課題】しかし、前記パブリックキー暗号化方式は、高速暗号化には不適であるという短所がある。尚、ＣＡシステムは不法視聴を防止することを目的とするが、しかし、ディジタルＶＣＲのようなＤＳＭを介して配布されるプログラムに対しては、不法複写に対して保護する方法がなかった。

【００３７】即ち、ＤＳＭのような記録媒体によって補給されるプログラムに対する保護は、不法複写の防止を意味するが、既存のアナログＶＣＲシステムに適用された複写防止(Copy Protection)方式は、ディジタル方式の記憶媒体に適用し難く、且つ今までＤＳＭのための複写防止方式に対する研究は別に進んでいない。

【００３８】従って、本発明は、かかる問題点を解決するためのもので、その目的は、スクランブルされたビットストリームとスクランブリングに使用された暗号化されたキーを互いに異なる経路で伝送して、暗号化されたキーをスマートカードで復号した後、その情報に基づいて、ビットストリームをデスクランブルするようにし、ビットストリームのみでは正常的なデコードを行えない

ようにすることにより、不法視聴及び複写を防止するディジタル映像システムの不法視聴及び複写防止方法を提供することにある。

【００３９】このような本発明は、ＣＡシステムでスマートカードを導入して自動的に料金をチェック(checking)する機能を含んでＰＰＶ(Pay Per View)機能を一層強力にし、スマートカードの代替により多様な機能を追加することで、システムの性能を簡単にアップグレード(Upgrade)させることができる。

【００４０】尚、本発明は、伝送データを分離するので、保護するデータのキー分量を大幅減少することができ、パワーオン時もしくは録画のためのディジタルＶＣＲ間の連結時に、自動的に認証及びキー交換過程を行うので、不法スマートカードでは動作されなくて、保護機能の信頼性をさらに向上させることになる。

【００４１】

【課題を解決するための手段】本発明によるディジタル映像システムの不法視聴及び複写防止方法は、入力されるデータがスクランブル(scramble)されたかどうかを判別する判別段階と、前記判別段階でスクランブルされたデータと判別されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、キー情報に応じて前記分離されたビットストリームをデスクランブル(descramble)して、ディスプレイ装置にディスプレイする再生段階と、前記判別段階でスクランブルされたデータと判別されると、記録もしくは複写モードに応じてビットストリームとキーストリームが混合されたスクランブルされたデータ状態で記録媒体に記録したり、スクランブルされたデータをビットストリームとキーストリームに分離し、分離されたキーストリームを暗号化した後、ビットストリームと混合して記録媒体に記録する記録段階と、前記判別段階でスクランブルされたデータと判別されると、スクランブルされたデータをビットストリームとキーストリームに分離した後、「ＰＰＣ」モードもしくは「バックアップ・コピー(Back-up Copy)」モードに応じて分離されたキーストリームを記録側のキー情報に対して復号化して伝送したり、分離されたキーストリームを自身のキー情報と記録側のキー情報に対して２回復号化して伝送する伝送段階とからなり、前記再生段階、記録段階、伝送段階は、同時又は選択的に行うことができており、そのことにより上記目的が達成される。

【００４２】ある実施形態では、前記判別段階でスクランブルされていないデータと判別されると、スクランブルされていないデータは不法視聴及び複写防止機能を適用しない。

【００４３】ある実施形態では、前記再生段階は、分離されたキーストリームをＭＰＥＧビットストリームに対する復号化アルゴリズムで復号化して、キー情報を判読する。　ある実施形態では、前記記録段階の複写動作は、キーストリームを自身のキー情報に対して暗号化する第１段階と、第１段階で暗号化されたキーストリームが「ＰＰＣ」モードであるか、或いは「バックアップ・コピー」モードであるかを判別する第２段階と、前記第２段階で「ＰＰＣ」モードと判別されると、記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第３段階と、前記第２段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して復号化されて伝送されたキーストリームを記録側のキー情報に対して暗号化し、その自身のキー情報に対して復号化した後、インデックスコードに対応する位置に挿入してビットストリームのように記録する第４段階と、からなっている。

【００４４】ある実施形態では、前記第３段階の「ＰＰＣ」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第１伝送段階と、前記第１伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、記録側のキー情報に対して復号化して伝送する第２伝送段階と、前記第２伝送段階で伝送されたキーストリームをインデックスコードに対応して記録側のキー情報に対して暗号化した後、前記第１伝送段階で伝送されたビットストリームに混合して記録媒体に記録する記録段階と、からなっているある実施形態では、前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+E^{G}(KS)$)をビットストリーム($S_{KS}(BS)$)とキーストリーム($E^{G}(KS)$)に分離した後、キーストリーム($E^{G}(KS)$)が分離された部分にインデックスコードＩＤＸを挿入する分離段階と、前記分離段階で分離されたキーストリーム($E^{G}(KS)$)を自身のキー情報に対して暗号化する暗号化段階と、前記暗号化段階で暗号化されたキーストリームを自身のキー情報とＭＰＥＧビットストリームに対して復号化することによりキー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて前記分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルする復号化段階と、を含んでいる。

【００４５】ある実施形態では、前記第４段階の「バックアップ・コピー」モード動作は、ビットストリームとキーストリームを分離した後、そのキーストリームが分離された部分にインデックスコードを挿入して伝送する第１伝送段階と、前記第１伝送段階で分離されたキーストリームを自身のキー情報に対して暗号化した後、暗号化されたキーストリームを記録側のキー情報と自身のキー情報に対して復号化して伝送する第２伝送段階と、前記第２伝送段階で伝送されたキーストリームをインデックスコードに対応して、記録側のキー情報に対して暗号

化した後、前記第１伝送段階で伝送されたビットストリームに混合して、記録媒体に記録する記録段階と、からなっている。

【００４６】ある実施形態では、前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+D^{SC}_{AK}[E^{G}(KS)]$)を、ビットストリーム($S_{KS}(BS)$)とキーストリーム($D^{SC}_{AK}[E^{G}(KS)]$)を分離した後、キーストリーム($D^{SC}_{AK}[E^{G}(KS)]$)が分離された部分に、インデックスコードＩＤＸを挿入する分離段階と、前記分離段階で分離されたキーストリーム($D^{SC}_{AK}[E^{G}(KS)]$)を自身のキー情報に対して２回暗号化する暗号化段階と、前記暗号化段階において、２回暗号化されたキーストリームを自身のキー情報とＭＰＥＧビットストリームに対して復号化することにより、キー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて、分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルする復号化段階と、を含んでいる。

【００４７】本発明によるディジタル映像システムの不法視聴及び複写防止方法は、スクランブルされたデータが入力されると、前記スクランブルされたデータをビットストリームとキーストリームに分離した後、分離されたキーストリームを復号してキー情報を判読し、判読されたキー情報に基づいて、前記分離されたビットストリームをデスクランブルして、ディスプレイ装置にディスプレイする再生段階と、スクランブルされたデータが入力されると、ビットストリームとキーストリームが混合されたスクランブルされたデータ状態で、記録媒体に記録する記録段階とからなり、前記再生段階、記録段階は、同時若しくは選択的に行うことができており、そのことにより上記目的が達成される。

【００４８】ある実施形態では、前記再生段階は、分離されたキーストリームを、ＭＰＥＧビットストリームに対する復号化アルゴリズムで復号してキー情報を判読し、判読されたキー情報で、デスクランブル方式を判別する。

【００４９】ある実施形態では、前記記録段階で記録が終了して再生を行うと、再生されたビットストリーム($S_{KS}(BS)+E^{G}(KS)$)をビットストリーム($S_{KS}(BS)$)とキーストリーム($E^{G}(KS)$)に分離した後、キーストリーム($E^{G}(KS)$)が分離された部分に、インデックスコードＩＤＸを挿入する分離段階と、前記分離段階で分離されたキーストリーム($E^{G}(KS)$)を自身のキー情報に対して、暗号化アルゴリズムで暗号化する暗号化段階と、前記暗号化段階で２回暗号化されたキーストリームを、自身のキー情報とＭＰＥＧビットストリームに対して復号化することにより、キー情報を判読する判読段階と、前記判読段階で判読されたキー情報に基づいて、前記分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルして、ディスプレイ装置にディスプレイする復号化段階と、を含んでいる。

【００５０】本発明によるディジタル映像システムの不法視聴及び複写防止方法は、複写時に自身のキー情報に対して暗号化されたキーストリームが伝送されると、「バックアップ・コピー」モードであるか、もしくは「ＰＰＣ」モードであるかを判別する判別段階と、前記判別段階で［ＰＰＣ」モードと判別されると、記録側のキー情報に対して前記キーストリームを復号化して伝送する第１伝送段階と、前記第１伝送段階で伝送されたキーストリームを記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入して、ビットストリームのように記録媒体に記録する第１記録段階と、前記判別段階で「バックアップ・コピー」モードと判別されると、自身のキー情報と記録側のキー情報に対して、キーストリームを２回復号化して伝送する第２伝送段階と、前記第２伝送段階で伝送されたキーストリームを、記録側のキー情報に対して暗号化した後、暗号化されたキーストリームをインデックスコードに対応する位置に挿入してビットストリームのように記録媒体に記録する第２記録段階と、からなっており、そのことにより上記目的が達成される。

【００５１】ある実施形態では、前記第１伝送段階は、自身のキー情報Ａｋに対して暗号化されたキーストリームを自身のキー情報Ａｋに対して復号化し、さらに記録側のキー情報ＡＩに対して復号化した後、伝送する。

【００５２】ある実施形態では、前記第２伝送段階は、自身のキー情報Ａｋに対して暗号化されたキーストリームを、自身のキー情報Ａｋに対して２回復号化し、さらに記録側のキー情報ＡＩに対して復号化した後伝送する。

【００５３】本発明によるディジタル映像システムの不法視聴及び複写防止方法は、記録媒体の再生時にキーストリーム($E^{G}(KS)$)が検出されると「ＰＰＣ」記録媒体と判別して、キーストリームを自身のキー情報に対して暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いて、ビットストリームをデスクランブルする「ＰＰＣ」モード再生段階と、記録媒体の再生時に自身のキー情報に対して復号化されたキーストリーム($D^{SC}_{AK}[E^{G}(KS)]$)が検出されると、「バックアップ・コピー」記録媒体と判別して、自身と記録側のキー情報に対して２回暗号化した後、自身のキー情報で復号してキー情報を判読し、判読されたキー情報とインデックスコードを用いてビットストリームをデスクランブルする「バックアップ・コピー」モード再生段階と、からなっており、そのことにより上記目的が達成される。

【００５４】本発明によるディジタル映像システムの不法視聴及び複写防止装置は、アナログ放送信号を変復調してＲＳデコードする復調及び誤り訂正手段と、前記復調及び誤り訂正手段の出力を記録／再生装置に伝送し、

その記録／再生装置で再生されるスクランブルされた記録信号をビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する複写防止処理手段と、前記復調及び誤り訂正手段若しくは複写防止処理手段から出力されるビットストリームをデスクランブリング情報に基づいてデスクランブルするデコーダ手段と、前記複写防止処理手段で暗号化されたキーストリームを復号して、前記デコーダ手段へデスクランブリング情報として出力するスマート手段と、から構成しており、そのことにより上記目的が達成される。

【００５５】ある実施形態では、前記復調及び誤り訂正手段が接続されたデコーダ手段をスマート手段に接続して、前記スマートカードで前記デコーダ手段のキーストリームを自身のキー情報で復号して、デスクランブリング情報を前記デコーダ手段へ出力することにより、不法視聴防止機能を行うように構成している。

【００５６】ある実施形態では、前記復調及び誤り訂正手段が接続された複写防止処理手段が、ディジタル記録／再生装置に接続されて初めて録画を行う。

【００５７】ある実施形態では、前記ディジタル記録／再生装置が接続された複写防止手段のキーストリームラインをスマートカードに接続するとともにビットストリームラインをデコーダ手段に接続し、前記複写防止処理手段とデコーダ手段を接続して、前記スマートカードが前記デコーダ手段のインデックスコードに対応する前記複写防止処理手段のキーストリームを自身のキー情報で復号して、前記デコーダ手段へ出力することにより、不法再生を防止する。

【００５８】ある実施形態では、前記複写防止処理手段は「ＰＰＣ」モードの記録媒体再生時にディジタル記録／再生装置の再生データから分離したキーストリームを自身のキー情報で暗号化して、スマートカードへ伝送する。

【００５９】ある実施形態では、前記複写防止処理手段は、「バックアップ・コピー」モードの再生媒体再生時にディジタル記録／再生装置の再生データから分離したキーストリームを、自身のキー情報で２回暗号化してスマートカードへ伝送する。

【００６０】ある実施形態では、前記複写防止処理手段は、スマートカード固有のキー情報を記憶するＲＡＭと、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、前記ＲＡＭのキー情報で前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサと、からなっている。

【００６１】ある実施形態では、前記スマートカードは、ビットストリムの為の復号化アルゴリズムプログラムを貯蔵する第１アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第２アルゴリズム貯蔵メモリと、自身のキー情報を貯蔵するＲＯＭと、他のスマートカードのキー情報を一時貯蔵するＲＡＭと、から構成している。

【００６２】本発明によるディジタル映像システムの不法視聴及び複写防止装置は、第１ディジタル記録／再生装置の再生データをビットストリームとキーストリームに分離した後、分離されたキーストリームを暗号化する第１複写防止処理手段と、前記第１複写防止処理手段で暗号化されたキーストリームを自身のキー情報と記録側のキー情報に対して復号化する第１、第２スマートカードと、前記第２スマートカードを介して伝送された前記第１スマートカードのキーストリームを自身のキー情報で暗号化した後、暗号化されたキーストリームを分離されたビットストリームとともに、第２ディジタル記録／再生装置へ出力して、記録媒体に記録する第２複写防止処理手段と、から構成しており、そのことにより上記目的が達成される。

【００６３】ある実施形態では、前記第１複写防止処理手段は、キーストリームを自身のキー情報Ａｋに対して暗号化した後、第１スマートカードへ伝送する。

【００６４】ある実施形態では、前記第１スマートカードは、「ＰＰＣ」モードである時、第１複写防止処理手段のキーストリームを自身のキー情報と記録側のキー情報に対して復号化した後、第２スマートカードへ伝送する。

【００６５】ある実施形態では、前記第２複写防止処理手段は、第２スマートカードで伝送されるキーストリームを、自身のキー情報ＡＩに対して暗号化した後、第１複写防止処理手段のビットストリームと混合する。

【００６６】ある実施形態では、前記第１スマートカードは「バックアップ・コピー」モードであるとき、第１複写防止処理手段のキーストリームを、自身のキー情報に対して２回復号した後、記録側のキー情報に対して復号する。

【００６７】ある実施形態では、前記第２複写防止処理手段は、第２スマートカードから伝送されるキーストリームを自身のキー情報に対して暗号化し、その暗号化されたキーストリームをビットストリームと混合する。

【００６８】ある実施形態では、前記第１、第２複写防止処理手段は、スマートカード固有のキー情報を貯蔵するＲＡＭと、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵メモリと、前記ＲＡＭのキー情報によって、前記アルゴリズム貯蔵メモリの暗号化プログラムを実行するプロセッサと、から構成している。

【００６９】ある実施形態では、前記第１、第２スマートカードは、ビットストリームのための復号化アルゴリズムプログラムを貯蔵する第１アルゴリズム貯蔵メモリと、自身の復号化アルゴリズムプログラムを貯蔵する第２アルゴリズム貯蔵メモリと、自身のキー情報を貯蔵するＲＯＭと、他のスマートキー情報を一時貯蔵するＲＡＭと、から構成している。

【００７０】

【発明の実施の形態】以下、本発明を添付図面を参照して詳細に説明する。

【００７１】本発明はディジタル信号を記録及び再生し得る全ての記録／再生装置に適用可能であり、本発明では説明の便宜のためにＤＶＣＲを一実施例としている。

【００７２】従って、本発明の実施例は図７に示すように、アナログの放送信号を変復調してＲＳデコードする復調及び誤り訂正部１と、デスクランブリング情報に基づいて前記復調及び誤り訂正部１の出力をデスクランブルするＡＴＶデコーダ２と、スクランブルされた記録信号をビットストリームとキーストリームに分離し、分離されたキーストリームを暗号化する複写防止処理部４と、この複写防止処理部４で分離されて暗号化されたキーストリーム及び前記ＡＴＶデコーダ２のインデックスコードを復号して前記ＡＴＶデコーダ２にデスクランブリング情報ＫＳを出力するスマートカード３とから構成する。

【００７３】前記複写防止処理部４は図８に示すように、スマートカード固有のキー情報を貯蔵するＲＡＭ１７と、暗号化アルゴリズムを貯蔵するアルゴリズム貯蔵部１８と、前記ＲＡＭ１７のキー情報で前記アルゴリズム貯蔵部１８の暗号化プログラムを実行するプロセッサ１６とから構成する。

【００７４】前記スマートカード３は図９に示すように、ビットストリームのための復号化アルゴリズムを貯蔵する第１アルゴリズム貯蔵部１２と、自身の復号化アルゴリズムを貯蔵する第２アルゴリズム貯蔵部１３と、自身のキー情報を貯蔵するＲＯＭ１４と、他のスマートカードのキー情報を一時貯蔵するＲＡＭ１５と、前記ＲＯＭ１４若しくはＲＡＭ１５に貯蔵されたキー情報に対して前記第１、第２アルゴリズム貯蔵部１２、１３の貯蔵アルゴリズムで暗号化若しくは復号化を実行するプロセッサ１１とから構成する。

【００７５】この際、前記プロセッサ１１、１６はワイヤドロジック(Wired Logic)で構成するか、或いはマイクロプロセッサを用いることができ、マイクロプロセッサを用いる場合、スマートカードのための暗号化アルゴリズムはプログラムで内蔵することになる。

【００７６】以下、このように構成した本発明の動作及び作用効果を説明する。

【００７７】本発明でＭＰＥＧビットストリームが図１１（ａ）乃至（ｃ）のようなフォーマットで伝送されるが、図１１（ａ）はスクランブルされていないフォーマットであり、図１１（ｂ）はビットストリームに対してスクランブルされたフォーマットであり、図１１（ｃ）はビットストリームが選択的にスクランブルされたフォーマットである。

【００７８】本発明ではＭＰＥＧビットストリームに対してスクランブルされた場合、どんな形態でも保護(protection)が加わると前提する。

【００７９】従って、複写防止処理部４に図１１（ｂ）若しくは（ｃ）のようなフォーマットのスクランブルされたストリームデータ($S_{KS}(BS)+E^{G}(KS)$)が入力された場合、図１０に示すようにスプリッタ(Splitter)で図１１（ｄ）乃至（ｅ）のようなビットストリーム($S_{KS}(BS)+IDX$)とキーストリーム($E^{G}KS$)に分離し、記録モードを行うと、前記分離されたキーストリーム($E^{G}(KS)$)はさらに暗号化されてスマートカード３へ伝送される。

【００８０】ここで、図１１（ｃ）に示すように、ビットストリームが部分的にスクランブルされた場合には、スクランブルされた部分に対してのみ不法視聴及び複写防止機能を適用するので、部分的な保護機能を行うことができる。

【００８１】まず、図１１（ａ）に示すように、スクランブルされていないビットストリームが伝送された場合、復調及び誤り訂正部１で変復調及び復号されたビットストリームが複写防止処理部４に入力されてもスマートカード３へデータを伝送せず、前記復調及び誤り訂正部１のビットストリームが入力されたＡＴＶデコーダ２も前記スマートカード３にデータを伝送することなくビットストリームを復号する。従って、視聴及び複写に何の制限もなくなる。

【００８２】ここで、チューナから復調及び誤り訂正部１に入力される信号とＡＴＶデコーダ２から出力されるビデオ及びオーディオ信号はアナログ信号である。チューナから出力される信号は、ＧＡビットストリームからのＶＳＢ変調された信号である。そして、入出力信号のうち、ビットストリームとキーストリームはディジタルＤＶＣＲのためのディジタル信号である。この際、記録を行うと、ディジタルＶＣＲにビットストリームが記録され、この記録されたビットストリームは一般的なディジタルＶＣＲで再生される。つまり、スクランブリングがかからないＭＰＥＧビットストリームが複写防止処理部４に入力されて、図１０に示すようにスプリッタを通過してもキー情報が無いためにスマートカード３へ伝送されるデータが無いので、スクランブリングがかからない場合には、視聴及び複写に何の制限もない。

【００８３】尚、本発明は、録画若しくは複写防止機能を行う場合、ビットストリームとキーストリームに分離されて、それぞれ異なるラインで伝送されるが、複写防止方法に関する情報はＰＥＳヘッダ内の付加複写情報(Additional Copy Info.)フィルドに載せられて伝送される。

【００８４】この際、暗号化されたキーがないスクランブルされたビットストリームを、パブリックチャンネルで伝送しても、キーに関する情報が除去された状態なので、不法使用者に流出した場合には、碌にデスクランブリングを行うことができない。そして、分離されたキーはさらに暗号化されて伝送されるので、復号アルゴリズムがない場合には、ビットストリームをデスクランブル

することができない。従って、本発明はかかる不法視聴及び複写防止のためにＭＰＥＧ伝送プロトコルで任意のフィルドを用いるが、スクランブルされたビットストリームは、複写防止機能が適用されたものである。

【００８５】まず、「Transport-scrambling-controlフィルド」を「Not Scrambled」モードに変えておけば、デコーダ２では、デスクランブリングを行わないので、不法使用者は前記フィルドを操作することができない。このような複写防止方法は、「Transport-scrambling-controlフィルド」によって複写防止されるようにするか、或いは複写可能(free-copy)となるようにするかを決定するので、不法使用者はこのフィルドを操作することだけでは、複写防止機能を解除することができない。

【００８６】次に、不法使用者がＰＥＳヘッダ内の「付加複写情報(Additional Copy Info.)フィルド」を修正する方法で、このフィルドの修正は保護方法を変換させるものであって、保護方法自体を解体するものではないので、複写防止機能に大きな損傷を与えない。

【００８７】このような特徴を有する本発明によって支援される複写防止方法は、ＣＡ機能であるＰＰＶ(Pay Per View)、ＰＰＰ(Pay Per Play)機能をデフォールト(Default)とし、「No Copy」方法、「PPC(Pay Per Copy)」方法、「Back-up Copy」方法がある。

【００８８】ここで、「No Copy」方法は、他のビデオテープで複写を全くできないようにする方法であり、「PPC」方法は、１回複写ごとに料金を受けるものであり、「Back-up Copy」方法は、一側のディジタルＶＣＲで再生されるビデオテープを他側のディジタルＶＣＲで複写した時に複写されたビデオテープは一側のディジタルＶＣＲでのみ正常的に表示可能であり、他側のディジタルＶＣＲでは表示し得ない方法である。

【００８９】以下、本発明の複写防止方法及びそれによるＭＰＥＧビットストリームの流れを図１９乃至図２２を参照して説明する。

【００９０】図１９および２０は、記録若しくは再生モード時に複写防止処理部の動作に対する信号流れ図であり、図２１は前記複写防止処理部に対応するスマートカードの動作に対する信号流れ図であり、図２２は記録若しくは再生動作時のキー交換及び認証過程に対する信号流れ図である。

【００９１】まず、図１９の信号流れを説明する。ビットストリームが入力された複写防止処理部４は、キー情報の有無を確認してスクランブリングの如何を判別し、キー情報があってスクランブルされた場合、最初の録画であるか或いは複写録画であるかを判別する（Ｓ１０１）。

【００９２】即ち、スクランブルされたデータの場合、ビットストリーム($S_{KS}(BS)$)とキーストリーム($E^{G}(KS)$)の分離によって$S_{KS}(BS)$+IDX形態のストリームで伝送されるかどうかを検索して、$S_{KS}(BS)$+IDX形態のストリームが検出されると複写録画と判別し、検出されなければ最初の録画と判別する（Ｓ１０２）。

【００９３】これにより、最初録画と判別された場合、ＶＣＲ５でビットストリームとキーストリームが混合されたストリーム($S_{KS}(BS)+E^{G}(KS)$)をテープに録画し（Ｓ１０６）、複写録画と判別された場合、キーストリーム($E^{G}(KS)$)が分離されたビットストリーム($S_{KS}(BS)$+IDX)を記録側の複写防止処理部８に伝送するとともに、前記キーストリーム($E^{G}(KS)$)をキー情報Ａｋに対して、さらに暗号化した後（Ｓ１０５）、その暗号化されたキーストリーム($E^{SC_{Ak}}[E^{G}(KS)]$)をスマートカード３を介して、記録側のスマートカード７に伝送することにより、記録側のＶＣＲ９でテープに録画することになる（Ｓ１０６）。

【００９４】逆に、図２０は、図１９のような信号流れで録画をしたテープを再生する場合の信号流れ図である。複写防止処理部４は、ＶＣＲで再生されたビットストリームが入力されると（Ｓ１０７）、キーストリームを分離して判別することにより（Ｓ１０８）、録画機能が「Back-up Copy」であるかどうかを判別することになる（Ｓ１１０）。

【００９５】この際、前記段階（Ｓ１１０）はキー情報がなければ、一般的な録画テープと判別し、暗号化されたキーストリーム($E^{G}(KS)$)が検出されると最初録画テープと判別する。尚、自身のキー情報Ａｋに対して復号されたキーストリーム($D^{SC_{Ak}}[E^{G}(KS)]$)が検出されると、ＰＰＣ機能の録画テープと判別し、他のスマートカードのキー情報ＡＩに対して復号されたキーストリーム($D^{SC_{AI}}[E^{G}(KS)]$)が検出されると、「Back-up Copy」機能の録画テープと判別する。これにより、複写防止処理部４は、一般録がテープの場合には、ビットストリーム(BS)を、複写防止用録画テープの場合には、キーストリーム($E^{G}(KS)$)が分離されたビットストリーム($S_{KS}(BS)$+IDX)をデコーダ２に伝送する（Ｓ１０９）。

【００９６】そして、複写防止処理部４は複写防止用録画テープの再生時にBack-up Copy機能が適用された場合、キーストリーム($D^{SC_{Ak}}[E^{G}(KS)]$)を自身のキー情報Ａｋに対して暗号化アルゴリズム$E^{SC_{Ak}}(\cdot)$で２回暗号化することにより、暗号化されたキーストリーム($E^{SC_{Ak}}[E^{G}(KS)]$)をスマートカード３に伝送し（Ｓ１１１、Ｓ１１２、Ｓ１１３）、Back-up Copy機能が適用されていない場合、キーストリームム($E^{G}(KS)$)を自身のキー情報Ａｋに対して暗号化アルゴリズム($E^{SC_{Ak}}(\cdot)$)で暗号化することにより、暗号化されたキーストリーム($E^{SC_{Ak}}[E^{G}(KS)]$)をスマートカード３へ伝送する（Ｓ１１２、Ｓ１１３）。

【００９７】前記のような動作を複写防止処理部４で行うとき、スマートカード３は図２１のような信号流れの動作を行う。これを詳しく説明すると、前記スマートカード３は放送若しくは再生を行うことにより、デコーダ

２でインデックスコードＩＤＸ若しくはキーストリーム($E^{G}(KS)$)が入力されるかどうかを判別する（Ｓ１１４、Ｓ１１５）。

【００９８】この際、インデックスコードＩＤＸではないキーストリーム($E^{G}(KS)$)が入力されると、ＰＰＶ機能の放送視聴と判別したスマートカード３は、前記キーストリーム（$E^{G}(KS)$)をビットストリームＧＡに対する復号化アルゴリズムD^{G}（・）で復号して（Ｓ１１６）、キー情報ＫＳをデコーダ２に入力させる（Ｓ１１７）。これにより、デコーダ２はスマートカード３のキー情報ＫＳを判読してデスクランブリング方式を判別し、その判別されたデスクランブリング方式でビットストリーム（$S_{KS}(BS)$)をデスクランブルしてアナログビデオ信号及びオーディオ信号として出力することにより、視聴者は放送を視聴することができる。

【００９９】一方、前記段階（Ｓ１１５）でインデックスコードＩＤＸが入力されたと判別されると、スマートカード３は複写防止処理部４で入力されたキーストリーム($E^{SC_{Ak}}[E^{G}(KS)]$)をキー情報Ａｋに対して復号化アルゴリズム($D^{SC_{Ak}}(\cdot)$)で復号した後（Ｓ１１８）、再生動作か若しくは記録動作かを判別する（Ｓ１１９）。

【０１００】この際、前記段階（Ｓ１１９）で再生動作と判別されると、スマートカード３は復号化されたキーストリーム($E^{G}(KS)$)をビットストリームＧＡに対する復号化アルゴリズム($D^{G}(\cdot)$)で復号して（Ｓ１１６）、キー情報ＫＳをデコーダ２に入力させる（Ｓ１１７）。これにより、デコーダ２はスマートカード３のキー情報ＫＳを判読して、デスクランブリング方式を判別し、その判別されたデスクランブリング方式で複写防止処理部４で分離されたビットストリーム($S_{KS}(BS)$)をデスクランブルして、アナログビデオ信号及びオーディオ信号を出力することにより、視聴者はテープの録画プログラムを視聴することができる。

【０１０１】そして、前記段階（Ｓ１１９）で記録動作と判別されると、スマートカード３は「Back-up Copy」機能であるかどうかを判別する（Ｓ１２０）。「Back-up Copy」機能であれば、キーストリーム($E^{G}(KS)$)をキー情報Ａｋに対して、復号化アルゴリズム($D^{SC_{Ak}}(\cdot)$)で復号化し（Ｓ１２１）、復号化されたキーストリーム（($D^{SC_{Ak}}[E^{G}(KS)]$)をキー情報ＡＩに対して、復号化アルゴリズム($D^{SC_{Ak}}(\cdot)$)で復号化することになる（Ｓ１２２）。

【０１０２】この際、スマートカード３で復号化されたキーストリーム($D^{SC_{AI}}\{D^{SC_{Ak}}[E^{G}(KS)]\}$)が記録側に伝送され（Ｓ１２３）、スマートカード７を介して複写防止処理部８に入力されると（Ｓ１２４）、暗号化アルゴリズム($E^{SC_{AI}}(\cdot)$)で暗号化される。これにより、スマートカード７は暗号化されたキーストリーム($D^{SC_{Ak}}[E^{G}(KS)]$)をインデックスコードＩＤＸが指定する位置に混入させて再生側の複写防止処理部４から出力されたビットストリーム($S_{KS}(BS)$)と混合すると、ＶＣＲ９でテープに録画することになる。

【０１０３】一方、前記段階（Ｓ１１９）で記録動作と判別され、且つ前記段階（Ｓ１２０）で「Back-up Copy」機能ではないＰＰＣ機能が適用されたと判別されると、スマートカード３は、キーストリーム($E^{G}(KS)$)をキー情報ＡＩに対して復号化アルゴリズム($D^{SC_{AI}}(\cdot)$)で復号化し（Ｓ１２２）、その復号化されたキーストリーム($D^{SC_{AI}}[E^{G}(KS)]$)を記録側へ伝送することになる（Ｓ１２３）。

【０１０４】この際、スマートカード７を介してキーストリーム($D^{SC_{AI}}[E^{G}(KS)]$)の入力を受けた記録側の複写防止処理部８は、暗号化アルゴリズム$E^{SC_{AI}}$（・）で暗号化した後、その暗号化されたキーストリーム($E^{G}(KS)$)をインデックスコードＩＤＸが指定する位置に混入させて、再生側の複写防止処理部４から出力されたビットストリーム($S_{KS}(BS)$)と混合することになる。

【０１０５】従って、複写防止処理部８から出力されたビットストリーム($S_{KS}(BS)+E^{G}(KS)$)はＶＣＲ９によってテープに録画される。

【０１０６】上述したように、本発明では全てのスマートカードがＭＰＥＧビットストリームに対する暗号化アルゴリズム($E^{G}(\cdot)$)と復号化アルゴリズム($D^{G}(\cdot)$)に対して共通のアルゴリズム及び共通のキーを持つ。

【０１０７】そして、スマートカードに対する暗号化アルゴリズム($E^{SC_{AI}}(\cdot)$)と復号化アルゴリズム($D^{SC_{Ak}}(\cdot)$)は全てのスマートカードが共通のアルゴリズムを持つが、キー情報はスマートカードによって異なる。即ち、各スマートカードは自身の認識名ＩＤに該当する認証キーを内蔵することになる。

【０１０８】前記のような動作を行うに当たり、複写防止処理部とスマートカード間、スマートカードとスマートカード間に相手を認識し得る認証過程及びキーを交換する過程を含む処理化動作が必要である。この際、認証過程はＤＥＳアルゴリズムのような対称キーアルゴリズムを用いる方法や、ＲＳＡのようなパブリックキーアルゴリズムを用いる方法や、ＦＳ(Fiat-Shamir)Schemeを用いる方法等の多様な方法が提示されている。

【０１０９】本発明では、パブリックキーアルゴリズムを用いる認証過程を行うとともに、キーを交換する方法の例を図２２に示したが、このような方法はパブリックキー（ｎ、ｅ）を認証しようとするキー受信手段２０１とキー伝送手段２０２が共有しているという前提のもとで、適用することになる。

【０１１０】この際、キー受信手段２０１は複写防止処理部若しくは記録側のスマートカード１であり、キー伝送手段２０２は自身のスマートカードｋである。

【０１１１】以下、前記のような流れで動作する本発明の実施例を図１２乃至図１８を参照して説明する。

【０１１２】本発明では図１１（ａ）のようなスクラン

ブルされていないビットストリームＢＳが伝送された場合、図１２に示すように回路が動作するので、復調及び誤り訂正部１で変復調及びＲＳデコードされたビットストリームがデコーダ２で復号されるにより、アナログビデオ及びオーディオ信号が出力される。

【０１１３】この際、記録の場合、復調及び誤り訂正部１から出力されるビットストリームＢＳは、複写防止処理部４を介してＶＣＲ５でテープに記録され、再生の場合、ＶＣＲ５で再生されたビットストリームＢＳが複写防止処理部４を介してデコーダ２に入力されて復号されることによりアナログビデオ及びオーディオ信号が出力される。即ち、複写防止処理部４からスマートカード３へデータを出力しないので、視聴及び複写に影響を与えない。

【０１１４】そして、図１１（ｂ）又は（ｃ）のようなスクランブルされたビットストリームが入ってくる場合、ＣＡ機能を適用することにより、図１３において図１８のような動作を行う。

【０１１５】まず、ＰＰＶ機能を行う場合、図１３のような信号流れで動作するが、スクランブルされたビットストリーム（$S_{KS}(BS)$）と暗号化されたキーストリーム（$E^{G}(KS)$）が伝送されると、復調及び誤り訂正部１は変調された入力信号を復調した後、ＲＳデコーディングを介して伝送中に発生した誤りを訂正することになる。

【０１１６】この際、デコーダ２が復調及び誤り訂正部１の出力（$S_{KS}(BS)+E^{G}(KS)$）のうち、キーストリーム（$E^{G}(KS)$）を分離してスマートカード３へ出力すると、スマートカード３は前記暗号化されたキーストリーム（$E^{G}(KS)$）を復号してキーストリームＫＳを前記デコーダ２にさらに出力する。これにより、デコーダ２はスマートカード３のキーストリームＫＳを判読してデスクランブリング方式を判別した後、ビットストリーム（$S_{KS}(BS)$）を復号してアナログビデオ信号及びオーディオ信号を出力することになる。

【０１１７】ここで、図９のようなスマートカード３はプロセッサ１１が復号化アルゴリズム（$E^{G}(\cdot)$）で暗号化されたキーストリーム（$E^{G}(KS)$）を復号して、その復号されたキーストリームＫＳをデコーダ２へ出力することになる。

【０１１８】一方、スクランブルされたビットストリームを最初に録画する場合、図１４のような信号流れで動作するが、伝送されたビットストリーム（$S_{KS}(BS)+E^{G}(KS)$）は、復調及び誤り訂正部１で復調及びＲＳデコーディングを介して誤りが訂正された後、複写防止処理部４を介してＶＣＲ５に入力されてテープに録画される。

【０１１９】このように録画されたビットストリームを再生する場合、ＰＰＰ機能であるとき、図１５のような信号流れで動作するが、ＶＣＲ５で再生されたビットストリーム（$S_{KS}(BS)+E^{G}(KS)$）が複写防止処理部４に入力されると、複写防止処理部４は再生されたビットストリーム（$S_{KS}(BS)+E^{G}(KS)$）をビットストリーム（$S_{KS}(BS)$）とキーストリーム（$E^{G}(KS)$）に分離した後、前記分離されたキーストリーム（$E^{G}(KS)$）を暗号化アルゴリズム（$E^{SC_{Ak}}(\cdot)$）でさらに暗号化して、スマートカード３へ出力し、前記分離されたビットストリーム（$S_{KS}(BS)$）はキーストリーム（$E^{G}(KS)$）が取り出された部分にインデックスコードＩＤＸを負荷してデコーダ２へ出力する。

【０１２０】この際、デコーダ２を介してインデックスコードＩＤＸの入力を受けたスマートカード３は、複写防止処理部２の暗号化されたキーストリーム（$E^{SC_{Ak}}[E^{G}(KS)]$）をスマートカードのための復号化アルゴリズム（$D^{SC_{Ak}}(\cdot)$）で復号して、デスクランブリング情報であるキーストリームＫＳを前記デコーダ２へ出力する（Ｓ１１７）。これにより、デコーダ２はスマートカード３のキーストリームＫＳを判読してデスクランブリング方式を判別した後、複写防止処理部４を介して入力されたビットストリーム（$S_{KS}(BS)$）を復号することにより、アナログビデオ信号及びオーディオ信号を出力することになる。

【０１２１】そして、図１４のような信号流れで録画されたデータを異なるＶＣＲで録画する場合、図１６の信号流れのようにＰＰＣ機能を行うが、ＶＣＲ５で再生されたビットストリーム（$S_{KS}(BS)+E^{G}(KS)$）が複写防止処理部４に入力されると、複写防止処理部４は、ビットストリーム（$S_{KS}(BS)+E^{G}(KS)$）を、ビットストリーム（$S_{KS}(BS)$）と、キーストリーム（$E^{G}(KS)$）とに分離する。その後、前記分離されたキーストリームを暗号化アルゴリズム（$E^{SC_{Ak}}(\cdot)$）でさらに暗号化してスマートカード３へ出力し、前記分離されたビットストリーム（$S_{KS}(BS)$）とキーストリーム（$E^{G}(KS)$）が取り出された部分にインデックスコードＩＤＸを付加して記録側の複写防止処理部８へ出力することになる。

【０１２２】この際、再生側のスマートカード３は、複写防止処理部４で暗号化されたキーストリーム（$E^{SC_{Ak}}[E^{G}(KS)]$）をＲＡＭに貯蔵されたキー情報ＡＩに対して復号化アルゴリズム（$D^{SC_{AI}}(\cdot)$）で復号した後、その復号されたキーストリーム（$D^{SC_{AI}}[E^{G}(KS)]$）を記録側のスマートカード７へ出力することになる。これにより、記録側のスマートカード７が再生側のスマートカード３のキーストリーム（$D^{SC_{AI}}[E^{G}(KS)]$）の入力を受けて記録側の複写防止処理部８へ出力すると、前記複写防止処理部８は前記キーストリーム（$D^{SC_{AI}}[E^{G}(KS)]$）を暗号化して元の暗号化されたキーストリーム（$E^{G}(KS)$）に復元した後、インデックスコードＩＤＸによって再生側の複写防止処理部４から出力されたビットストリーム（$G_{KS}(BS)$）に混合してＶＣＲ５へ出力することにより、他のテープに録画することになる。

【０１２３】このような動作で録画されたテープのデータはＰＰＰ機能を適用して、図１５のような信号流れで再生することができる。尚、図１４のような信号流れで

録画されたデータを他のＶＣＲで録画する場合、図１７の信号流れのようにBack-upCopy機能を行うことができる。

【０１２４】つまり、ＶＣＲ５で再生されたビットストリーム（$S_{KS}(BS)+E^{G}(KS)$）が複写防止処理部４に入力されると、複写防止処理部４はビットストリーム（$S_{KS}(BS)$）とキーストリーム（$E^{G}(KS)$）に分離した後、前記分離されたキーストリームを暗号化アルゴリズム（$E^{SC_{Ak}}(\cdot)$）でさらに暗号化してスマートカード３へ出力し、前記分離されたビットストリーム（$S_{KS}(BS)$）はキーストリーム（$E^{G}(KS)$）が取り出された部分にインデックスコードＩＤＸを付加して記録側の複写防止処理部８へ出力することになる。

【０１２５】この際、再生側のスマートカード３は複写防止処理部４で暗号化されたキーストリーム（$E^{SC_{Ak}}[E^{G}(KS)]$）をＲＯＭに貯蔵された自身のキーＡｋに対して復号化アルゴリズム（$D^{SC_{Ak}}(\cdot)$）で２回復号化した後、さらにＲＡＭに貯蔵されたキー情報ＡＩに対して復号化アルゴリズム（$D^{SC_{AI}}(\cdot)$）で復号して、その復号されたキーストリーム（$D^{SC_{AI}}\{D^{SC_{Ak}}[E^{G}(KS)]\}$）を記録側のスマートカード７に出力することになる。これにより、再生側のスマートカード３のキーストリーム（$D^{SC_{AI}}\{D^{SC_{Ak}}[E^{G}(KS)]\}$）が記録側のスマートカード７を介して記録側の複写防止処理部８へ出力されると、複写防止処理部８は前記キーストリーム（$D^{SC_{AI}}\{D^{SC_{Ak}}[E^{G}(KS)]\}$）をキー情報ＡＩに対して暗号化することにより、元の暗号化キーストリーム（$D^{SC_{Ak}}[E^{G}(KS)]$）に復元する。そして、復元された暗号化キーストリーム（$D^{SC_{Ak}}[E^{G}(KS)]$）を、インデックスコードＩＤＸによって再生側の複写防止処理部４から出力されたビットストリーム（$G_{KS}(BS)$）に混合して、ＶＣＲ９へ出力して、他のテープに録画することになる。

【０１２６】ここで、料金は改善されたスマートカード３若しくは７で計数する。

【０１２７】このようなBack-up Copy機能を行って録画されたデータは元テープを録画したＶＣＲでのみ再生することができるが、正常的な再生の場合、図１８（ａ）のような信号流れで動作を行う。

【０１２８】つまり、ＶＣＲ５で再生されたビットストリーム（$S_{KS}(BS)+D^{SC_{Ak}}[E^{G}(KS)]$）が複写防止処理部４に入力されると、複写防止処理部４は、ビットストリーム（$S_{KS}(BS)$）とキーストリーム（$D^{SC_{Ak}}[E^{G}(KS)]$）に分離する。その後、前記分離されたキーストリーム（$D^{SC_{Ak}}[E^{G}(KS)]$）を暗号化アルゴリズム（$E^{SC_{Ak}}(\cdot)$）で２回暗号化して、スマートカード３へ出力し、前記分離されたビットストリーム（$S_{KS}(BS)$）は、キーストリーム（$D^{SC_{Ak}}[E^{G}(KS)]$）が取り出された部分に、インデックスコードＩＤＸを付加してデコーダ２へ出力する。

【０１２９】この際、デコーダ２を介してインデックスコードＩＤＸの入力を受けたスマートコード３は複写防止処理部２で暗号化されたキーストリーム（$E^{SC_{Ak}}[E^{G}(KS)]$）をスマートカードのための復号化アルゴリズム（$D^{SC_{Ak}}(\cdot)$）で復号して、デスクランブリング情報であるキーストリームＫＳを前記デコーダ２へ出力する。これにより、デコーダ２はスマートカード３のキーストリームＫＳを判読してデスクランブリング方式を判別した後、複写防止処理部４を介して入力されたビットストリーム（$S_{KS}(BS)$）を復号することにより、アナログビデオ信号及びオーディオ信号を出力することになる。

【０１３０】そして、最初録画されたＶＣＲではない他のＶＣＲで再生する非正常再生の場合、図１８（ｂ）のような信号流れで動作することになって、テープの再生が不可能となる。

【０１３１】つまり、テープ複写を行ったＶＣＲ９で複写テープを再生すると、複写防止処理部８では再生されたデータ（$S_{KS}(BS)+D^{SC_{Ak}}[E^{G}(KS)]$）をスプリッティング処理して、ビットストリーム（$S_{KS}(BS)+IDX$）を分離する。

【０１３２】この際、分離されたキーストリーム（$D^{SC_{Ak}}[E^{G}(KS)]$）は自身のキー情報ＡＩに対して暗号化された後、さらにキー情報ＡＩに対して暗号化（$E^{SC_{AI}}\{E^{SC_{AI}}(D^{SC_{Ak}}[E^{G}(KS)])\}$）されてスマートカード７へ伝送される。そして、スマートカード７はビットストリーム（$E^{SC_{AI}}\{E^{SC_{AI}}(D^{SC_{Ak}}[E^{G}(KS)])\}$）を復号できないので、デコーダ６にキー情報ＫＳを伝送しない。これにより、スマートカード７はビットストリーム（$S_{KS}(BS)$）をデスクランブルしないので、複写テープの再生が行われない。

【０１３３】一方、本発明の理解のために、本発明に使用された用語を定義すると、下記の通りである。

【０１３４】１）ＢＳ：スクランブルされていないＧＡビットストリーム

２）ＫＳ＝[K_0、K_1、K_2、・・・K_i、・・・K_n]：キーストリーム

ここで、ｎはスクランブリングに使用されたキーの総数

３）ＢＳ＝[BS_0、BS_1、BS_2、・・・、BS_i、・・・BS_n]：ビットストリーム

ここで、BS_iはＢＳの一つのセグメントとして、スクランブルする単位

４）S_{KS}（ＢＳ）：スクランブルされたＭＰＥＧビットストリーム

S_{KS}（ＢＳ）＝[SK_0（BS_0）、SK_1（BS_1）、・・・、SK_i（BS_i）、・・・SK_n（BS_n）]

５）Ｅ（・）＆Ｄ（・）：ＧＡでキーを暗号化及び復号化するに使用されたアルゴリズム

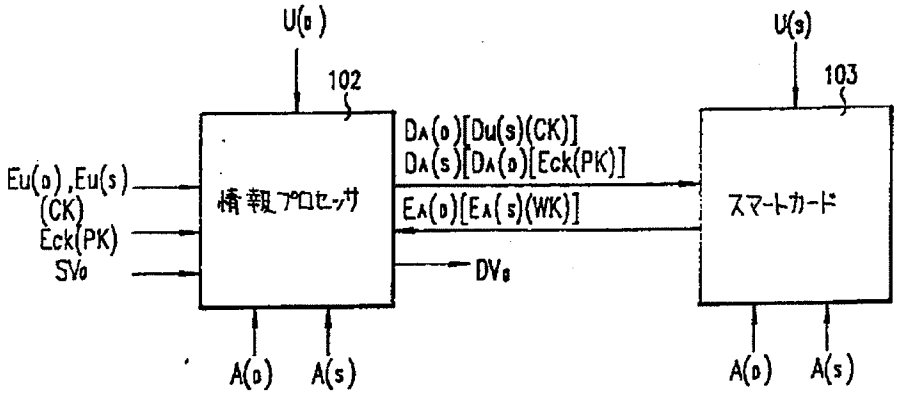
E^{G}（ＫＳ）＝[$E^{G}(K_0)$、$E^{G}(K_1)$、・・・、$E^{G}(K_i)$、・・・、$E^{G}(K_n)$]

D^{G}（ＫＳ）＝[$D^{G}(K_0)$、$D^{G}(K_1)$、・・・、$D^{G}(K_i)$、・・・、$D^{G}(K_n)$]＝ＫＳ

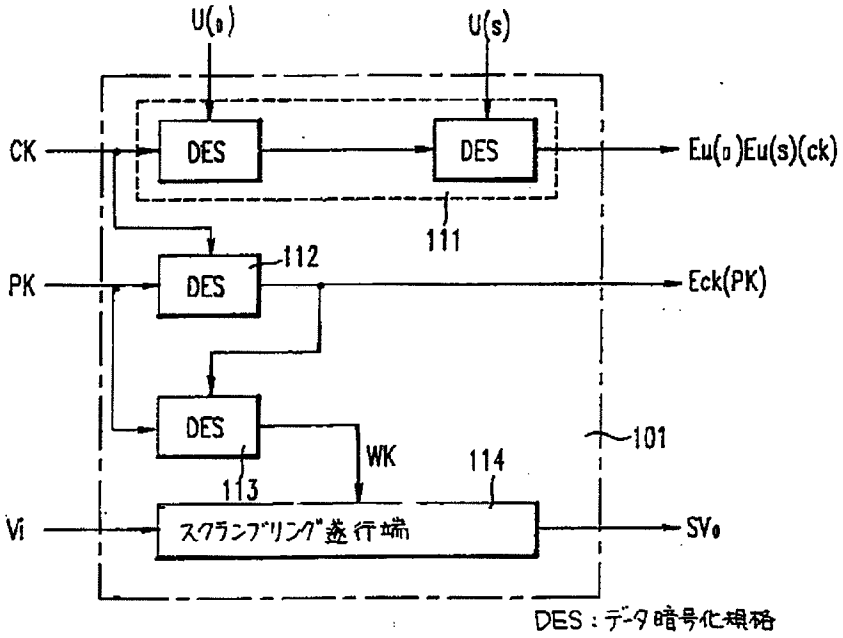
６）ＩＤＸ：[0、1、2、・・・、ｉ、・・・ｎ]：イ

ンデックスストリーム７）Ａｋ：スマートカード（ｋ）の認証キー
８）E^{SC_A}（・）＆D^{SC_A}（・）：スマートカードの認証キー（Ａ）をキーとしたスマートカードの暗号化及び復号化アルゴリズム。
【０１３５】
【発明の効果】以上説明したように、本発明はパワーオン時若しくはディジタルＶＣＲ間の連結時に、自動的に認証及びキー交換過程を行うので、不法スマートカードに対する不法視聴及び複写防止機能を自動的に行うことが出来、さらに部分的に不法視聴及び複写防止を行うことができるので、プログラムの保護を願う部分にスクランブリング処理を行うと、自動的に不法視聴及び複写防止を行いながら料金も所望通りに賦課することができる。
【０１３６】そして、本発明はビットストリームと分離させたキーストリームを異なるの経路で伝送するので、保護データの量を減少させることができて効率的に不法視聴及び複写防止機能を行うことができ、且つスマートカードに不法視聴防止と不法複写防止機能を具現するとき、ＰＰＶ、ＰＰＰ、ＰＰＣ及びBack-up Copy機能を区別するようにすることで、各機能に対して差別的に料金を賦課することができる。
【０１３７】尚、本発明はＤＳＭ応用に適用し得るディジタル信号の複写防止機能を具現することにより、ディジタルＶＣＲのようなＤＳＭにおけるプログラム著作権保護に適用することができる。従って、本発明を適用すると、不法視聴及び複写防止に対する信頼性を向上させることができるという効果が得られる。
【図面の簡単な説明】
【図１】一般的なスクランブラのブロック図である。
【図２】一般的なデスクランブラのブロック図である。
【図３】伝送フォーマットの例示図である。
【図４】図３におけるＰＥＳヘッダの詳細例示図である。
【図５】キー分配による伝送フォーマットの例示図である。
【図６】従来のＡＴＶデコーダのブロック図である。
【図７】本発明の不法視聴及び複写防止装置のブロック図である。
【図８】図７における複写防止処理部の詳細ブロック図である。
【図９】図７におけるスマートカードの詳細ブロック図である。
【図１０】図８におけるビットストリームのスプリッティング(splitting)を示す例示図である。
【図１１】(a)～(f)は、各ビットストリームのフォーマットを示す例示図である。
【図１２】本発明の接続状態を示す例示図である。
【図１３】本発明の接続状態を示す例示図である。
【図１４】本発明の接続状態を示す例示図である。
【図１５】本発明の接続状態を示す例示図である。
【図１６】本発明の接続状態を示す例示図である。
【図１７】本発明の接続状態を示す例示図である。
【図１８】本発明の接続状態を示す例示図である。
【図１９】本発明の動作のための信号流れ図である。
【図２０】本発明の動作のための信号流れ図である。
【図２１】本発明の動作のための信号流れ図である。
【図２２】本発明によるキー交換及び認証過程のための信号流れ図である。
【符号の説明】
１、１０４　復調及び誤り訂正部
２、６　ＡＴＶデコーダ
３　スマートカード
４、８　複写防止処理部
１１、１６　プロセッサ

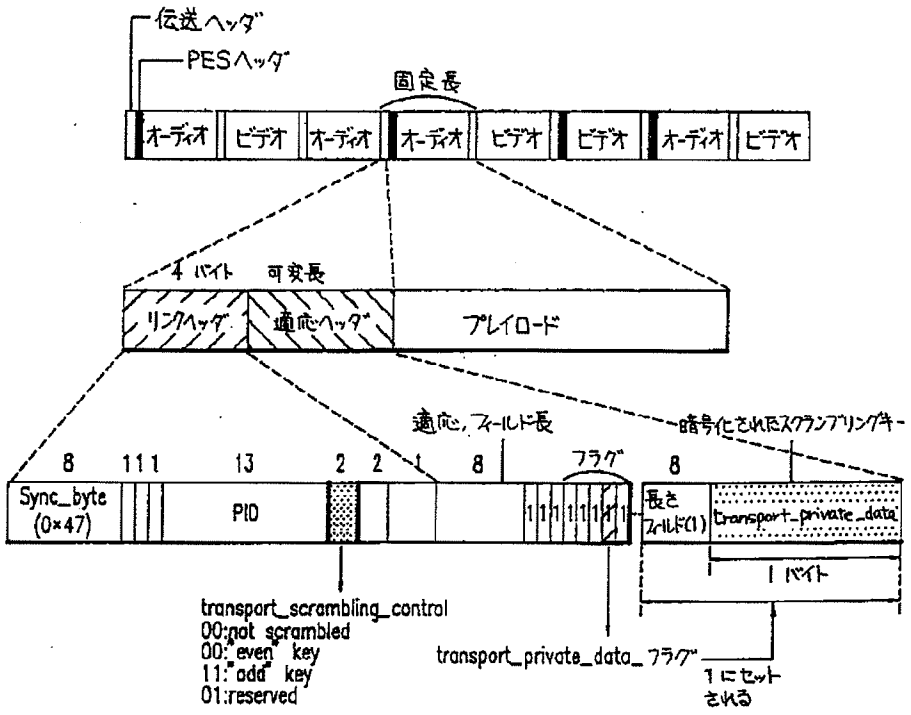
【図２】



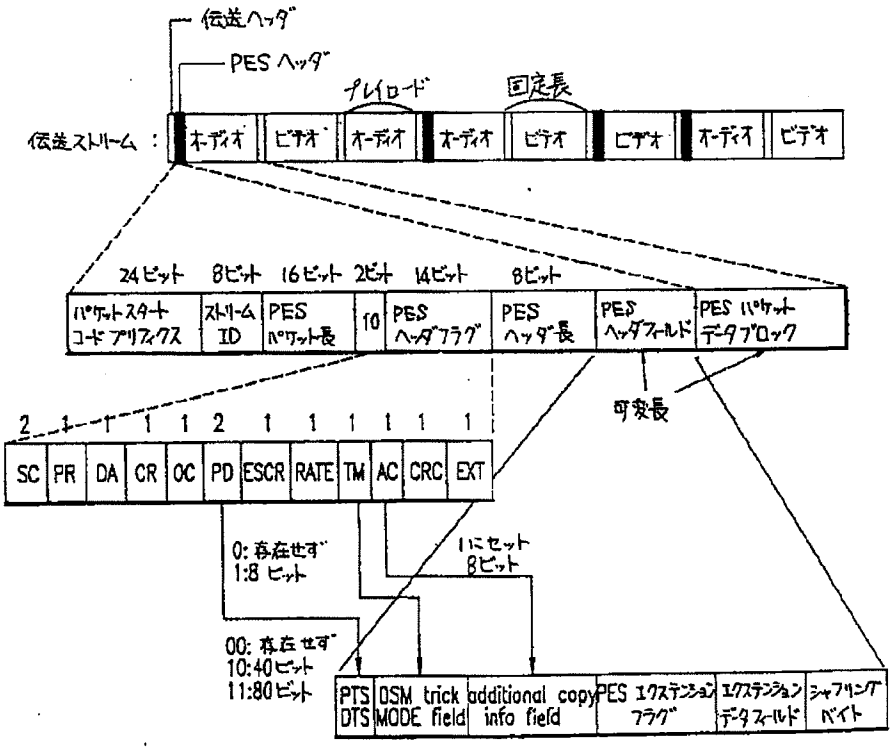
【図1】


U(0)
U(s)
CK
DES
DES
Eu(0)Eu(s)(ck)
111
PK
DES
112
Eck(PK)
DES
101
WK
114
113
Vi
スクランブリング遂行端
SV0
DES：データ暗号化規格

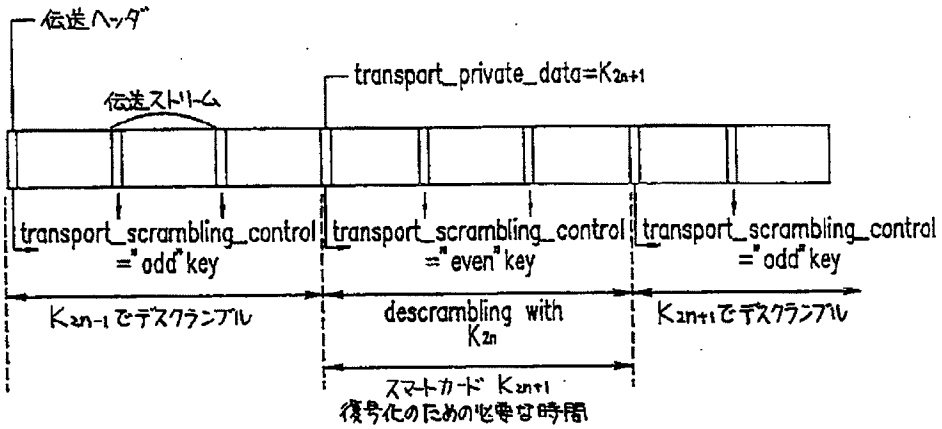
【図3】


伝送ヘッダ
PESヘッダ
固定長
オーディオ
ビデオ
オーディオ
オーディオ
ビデオ
ビデオ
オーディオ
ビデオ
4バイト
可変長
リンクヘッダ
適応ヘッダ
ペイロード
適応フィールド長
暗号化されたスクランブリングキー
フラグ
8
111
13
2
2
1
8
8
Sync_byte
(0×47)
PID
111111111
長さ
フィールド(1)
transport_private_data
1バイト
transport_scrambling_control
00:not scrambled
00:"even" key
11:"odd" key
01:reserved
transport_private_data_フラグ
1にセット
される

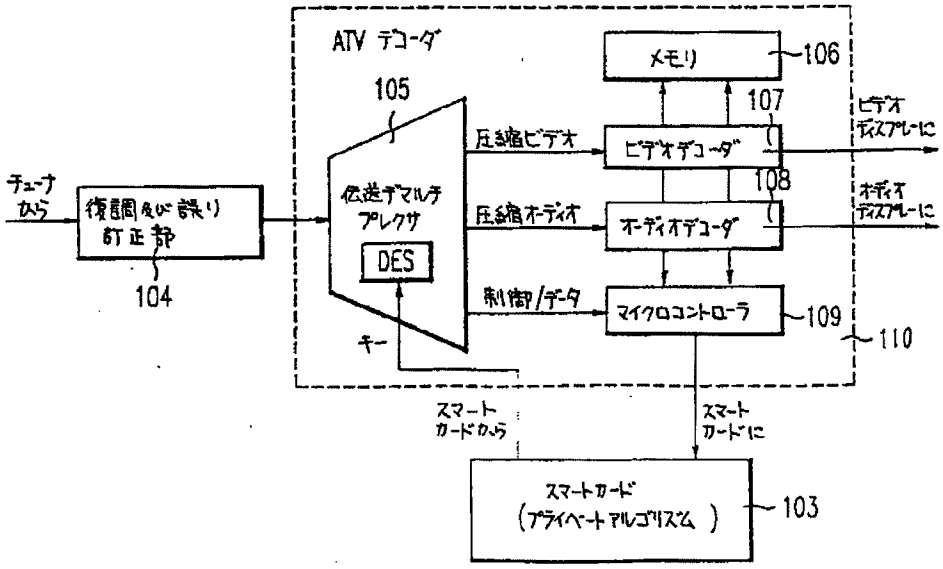
【図4】


伝送ヘッダ
PES ヘッダ
ペイロード
固定長
伝送ストリーム：
オーディオ
ビデオ
24ビット 8ビット 16ビット 2ビット 14ビット 8ビット
パケットスタートコードプリフィクス
ストリームID
PESパケット長
10
PESヘッダフラグ
PESヘッダ長
PESヘッダフィールド
PESパケットデータブロック
可変長
2 1 1 1 1 2 1 1 1 1 1 1
SC PR DA CR OC PD ESCR RATE TM AC CRC EXT
0: 存在せず
1:8ビット
1にセット
8ビット
00: 存在せず
10:40ビット
11:80ビット
PTS DTS
DSM trick MODE field
additional copy info field
PES エクステンションフラグ
エクステンションデータフィールド
シャフリングバイト

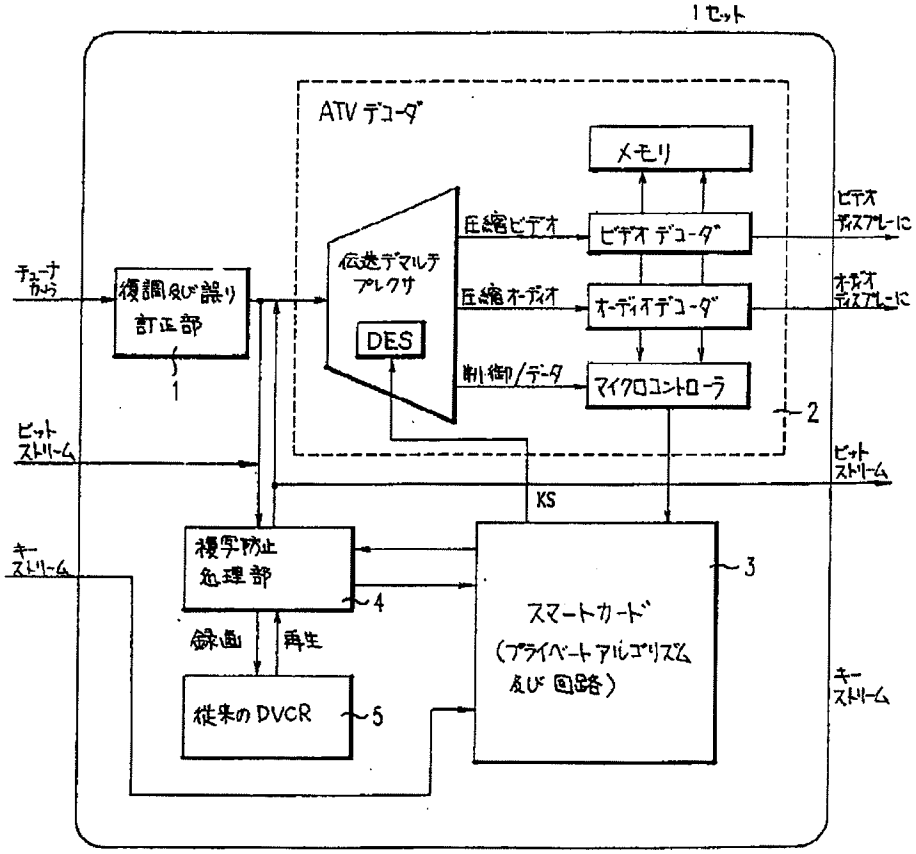
【図5】


伝送ヘッダ
伝送ストリーム
transport_private_data=K2n+1
transport_scrambling_control ="odd" key
transport_scrambling_control ="even" key
transport_scrambling_control ="odd" key
K2n-1でデスクランブル
descrambling with Kzn
K2n+1でデスクランブル
スマートカード K2n+1 復号化のための必要な時間

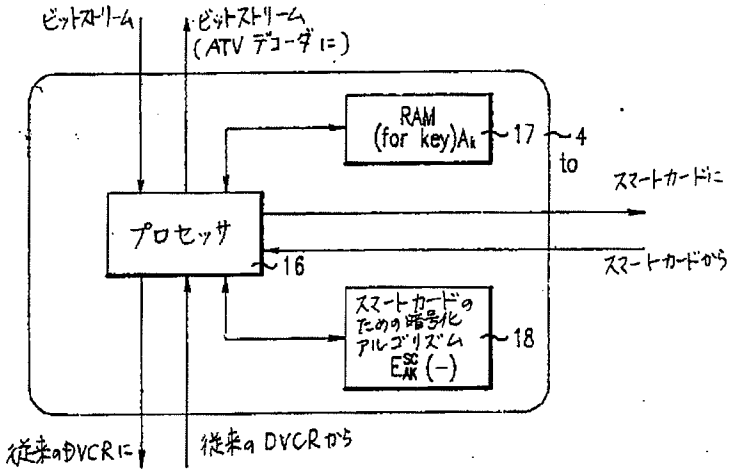
【図6】


ATV デコーダ
メモリ
106
105
107
ビデオディスプレーに
圧縮ビデオ
ビデオデコーダ
チューナから
復調及び誤り訂正部
伝送デマルチプレクサ
108
オーディオディスプレーに
圧縮オーディオ
オーディオデコーダ
DES
制御/データ
マイクロコントローラ
109
110
104
キー
スマートカードから
スマートカードに
スマートカード
(プライベートアルゴリズム)
103

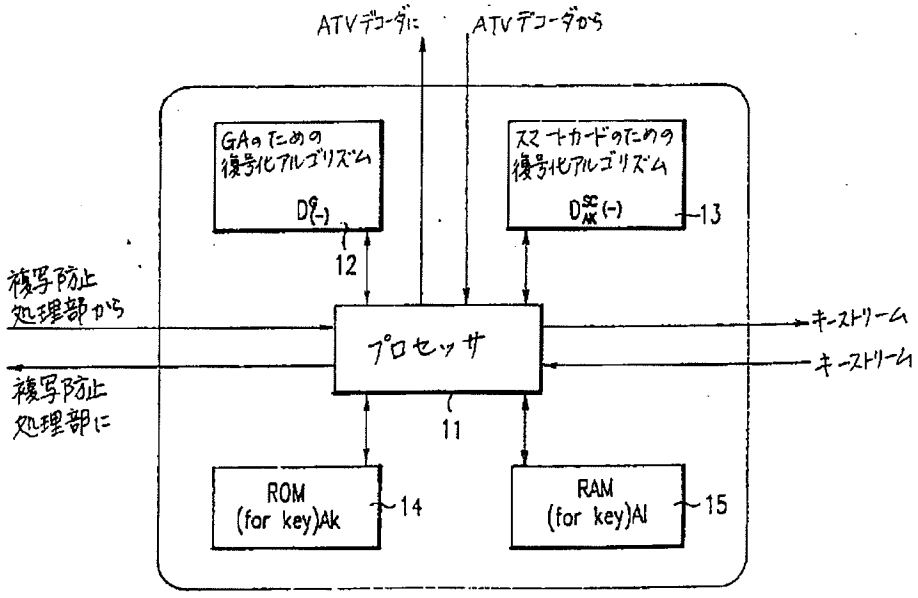
【図7】


1セット
ATV デコーダ
メモリ
ビデオディスプレーに
圧縮ビデオ
ビデオデコーダ
チューナから
復調及び誤り訂正部
伝送デマルチプレクサ
オーディオディスプレーに
圧縮オーディオ
オーディオデコーダ
DES
制御/データ
マイクロコントローラ
1
2
ビットストリーム
ビットストリーム
KS
キーストリーム
複写防止処理部
3
4
スマートカード
(プライベートアルゴリズム及び回路)
録画
再生
従来のDVCR
5
キーストリーム

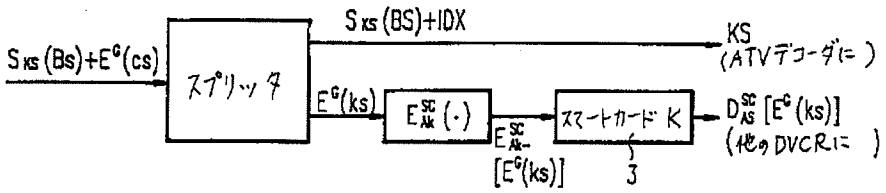
【図８】


ビットストリーム
ビットストリーム
(ATV デコーダに)
RAM
(for key)Ak
17
4
to
スマートカードに
プロセッサ
16
スマートカードから
スマートカードの
ための暗号化
アルゴリズム
18
従来のDVCRに
従来の DVCRから

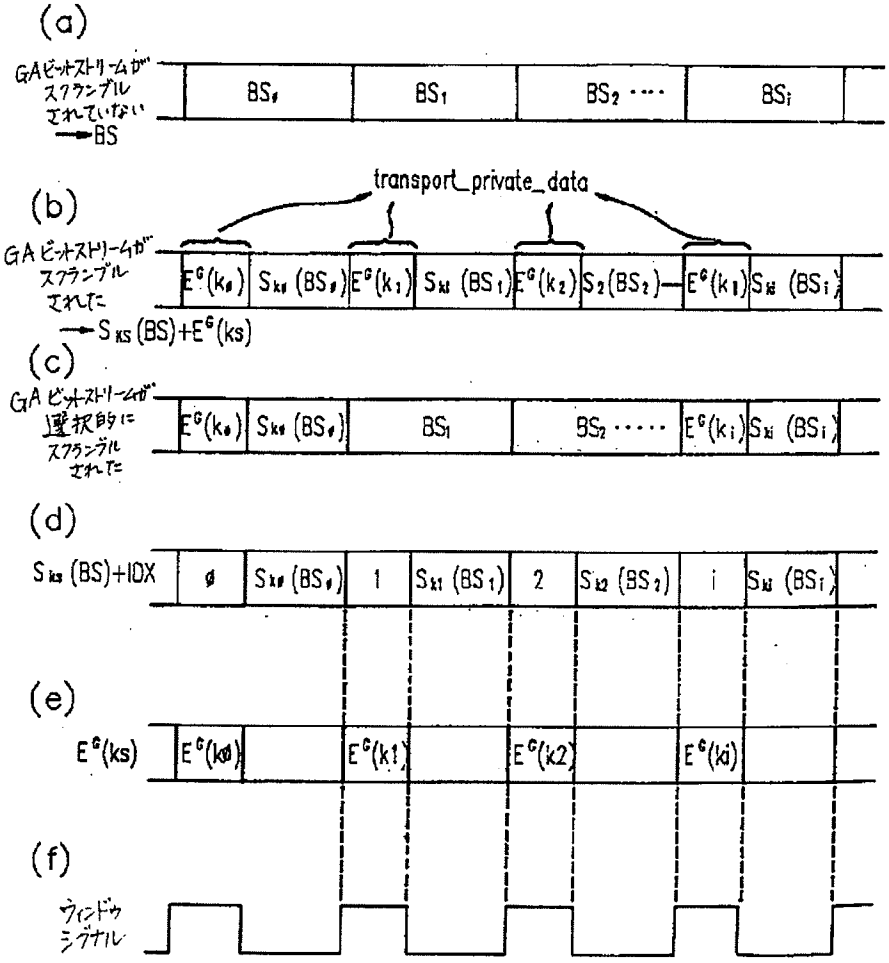
【図９】


ATVデコーダに
ATVデコーダから
GAのための
復号化アルゴリズム
スマートカードのための
復号化アルゴリズム
13
12
複写防止
処理部から
プロセッサ
キーストリーム
キーストリーム
複写防止
処理部に
11
ROM
(for key)Ak
14
RAM
(for key)AI
15

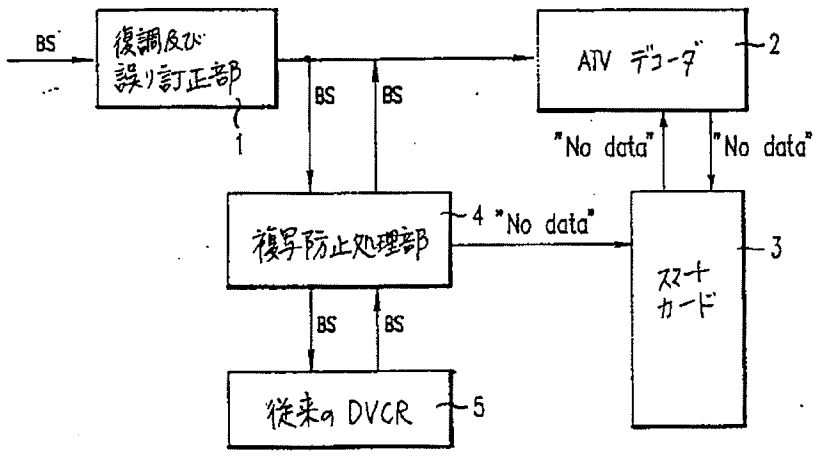
【図１０】


SKS(Bs)+EG(cs)
スプリッタ
SKS(BS)+IDX
KS
(ATVデコーダに)
EG(ks)
ESC AK(·)
スマートカード K
DSC AS[EG(ks)]
(他のDVCRに)
ESC AK[EG(ks)]
3

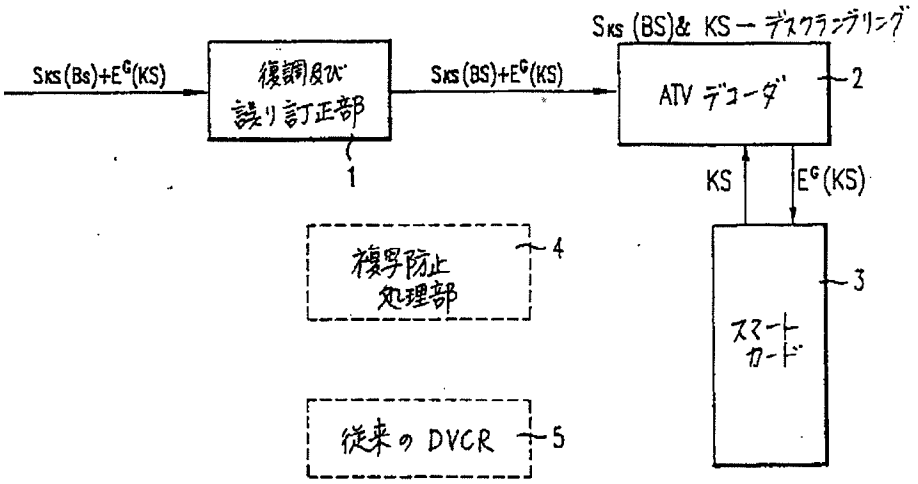
【図１１】


(a)
GAビットストリームがスクランブルされていない→BS
BS₀
BS₁
BS₂ ····
BSi
transport_private_data
(b)
GAビットストリームがスクランブルされた
→SKS(BS)+EG(ks)
EG(k₀)
SK₀(BS₀)
EG(k₁)
SK₁(BS₁)
EG(k₂)
S₂(BS₂)
EG(kᵢ)
Sᴋᵢ(BSᵢ)
(c)
GAビットストリームが選択的にスクランブルされた
EG(k₀)
SK₀(BS₀)
BS₁
BS₂ ·····
EG(kᵢ)
Sᴋᵢ(BSᵢ)
(d)
SKS(BS)+IDX
ø
SK₀(BS₀)
1
SK1(BS1)
2
SK2(BS2)
i
Sᴋᵢ(BSᵢ)
(e)
EG(ks)
EG(k0)
EG(k1)
EG(k2)
EG(ki)
(f)
ウィンドウシグナル

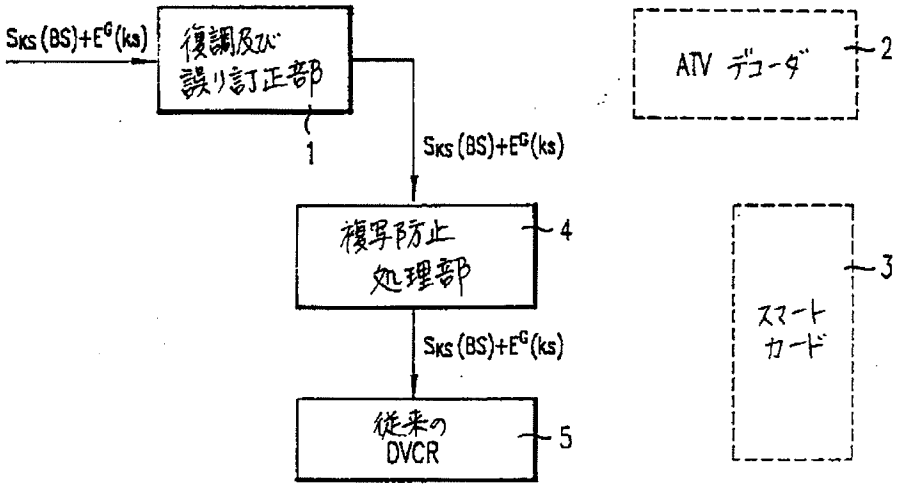
【図１２】


BS
復調及び誤り訂正部
1
BS
BS
ATV デコーダ
2
"No data"
"No data"
複写防止処理部
4 "No data"
スマートカード
3
BS
BS
従来のDVCR
5

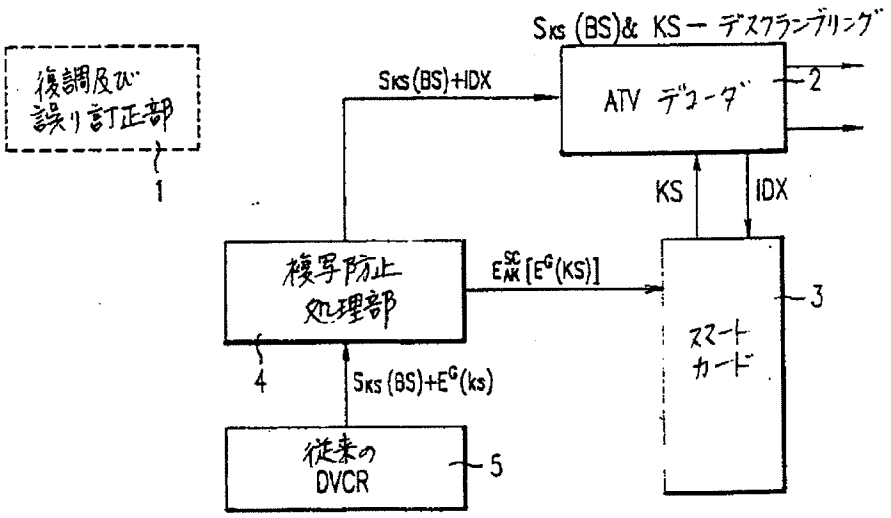
【図１３】


SKS(Bs)+E^G(KS)
復調及び
誤り訂正部
1
SKS(BS)+E^G(KS)
SKS(BS)& KS－デスクランブリング
ATV デコーダ
2
KS
E^G(KS)
3
スマート
カード
複写防止
処理部
4
従来の DVCR
5

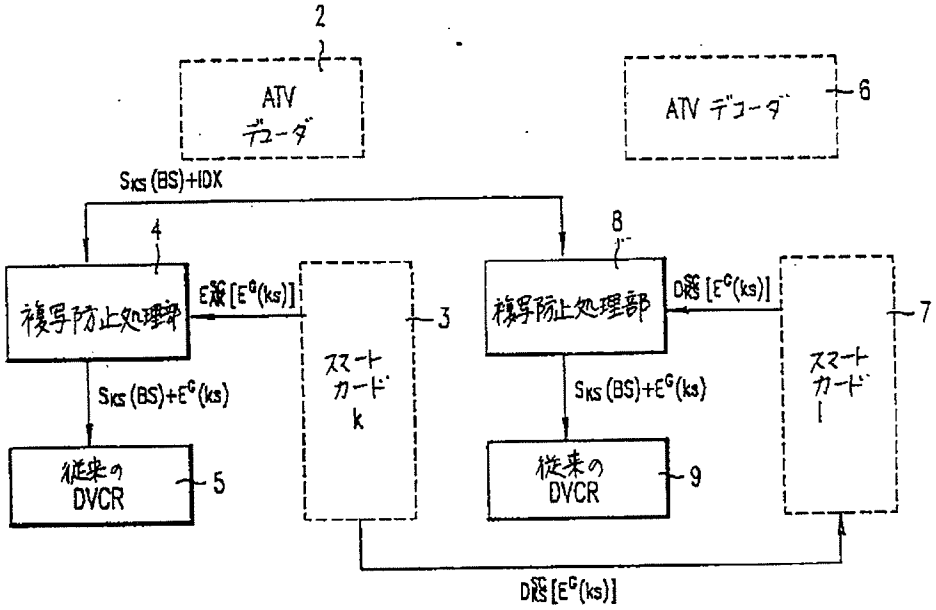
【図１４】


SKS(BS)+E^G(ks)
復調及び
誤り訂正部
1
SKS(BS)+E^G(ks)
ATV デコーダ
2
複写防止
処理部
4
SKS(BS)+E^G(ks)
3
スマート
カード
従来の
DVCR
5

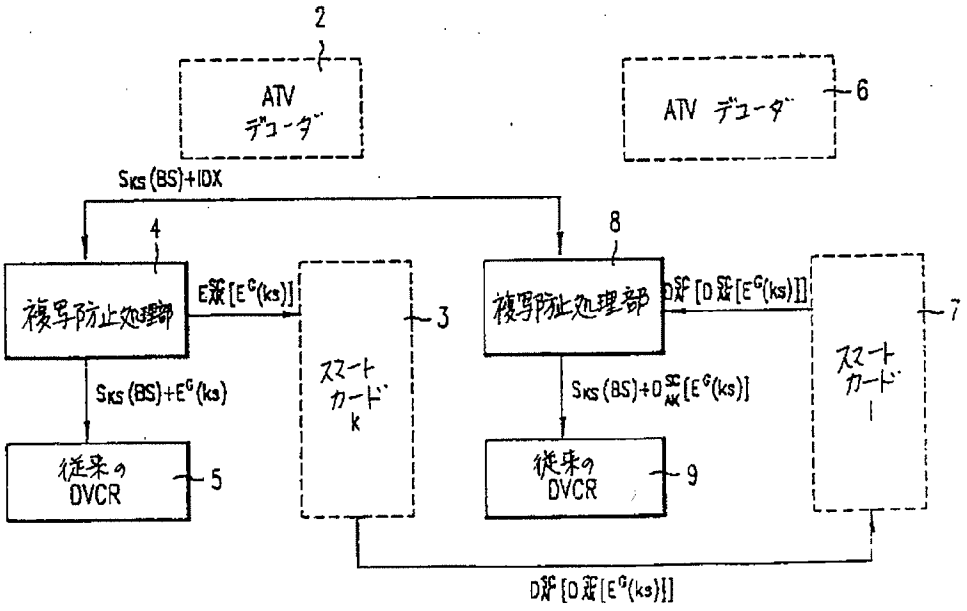
【図１５】


SKS (BS)& KS－ デスクランブリング
復調及び誤り訂正部
1
SKS(BS)+IDX
ATV デコーダ
2
KS
IDX
複写防止処理部
4
E^SC_AK[E^G(KS)]
3
スマートカード
SKS (BS)+E^G(ks)
従来のDVCR
5

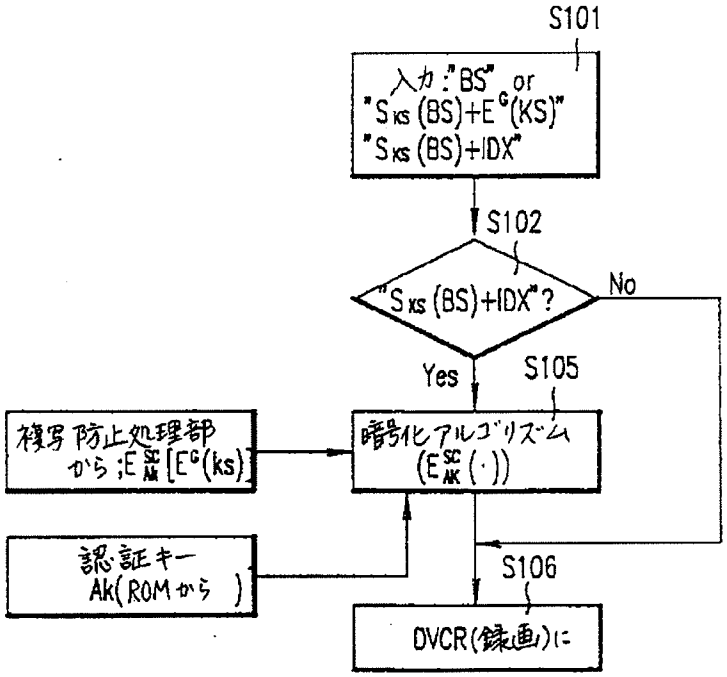
【図１６】


2
ATV デコーダ
ATV デコーダ
6
SKS (BS)+IDX
4
8
複写防止処理部
E鍵[E^G(ks)]
3
スマートカード k
複写防止処理部
D鍵[E^G(ks)]
7
スマートカード l
SKS (BS)+E^G(ks)
SKS (BS)+E^G(ks)
従来のDVCR
5
従来のDVCR
9
D鍵[E^G(ks)]

【図１７】

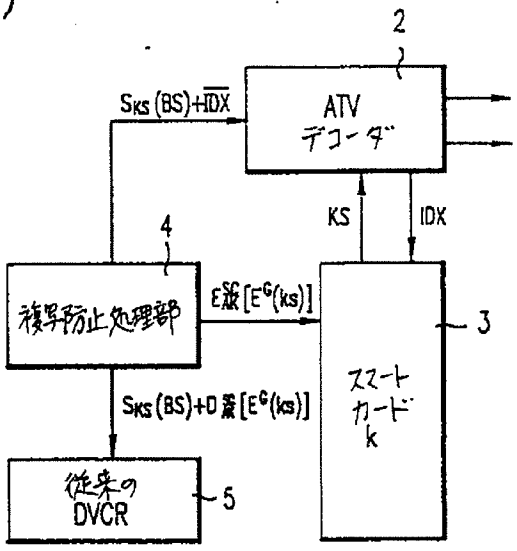

2
ATV デコーダ
ATV デコーダ
6
SKS(BS)+IDX
4
8
複写防止処理部
E鍵[E^G(ks)]
3
複写防止処理部
D鍵[D鍵[E^G(ks)]]
7
スマートカード k
スマートカード l
SKS(BS)+E^G(ks)
SKS(BS)+D^SC_AK[E^G(ks)]
従来の DVCR
5
従来の DVCR
9
D鍵[D鍵[E^G(ks)]]

【図１９】

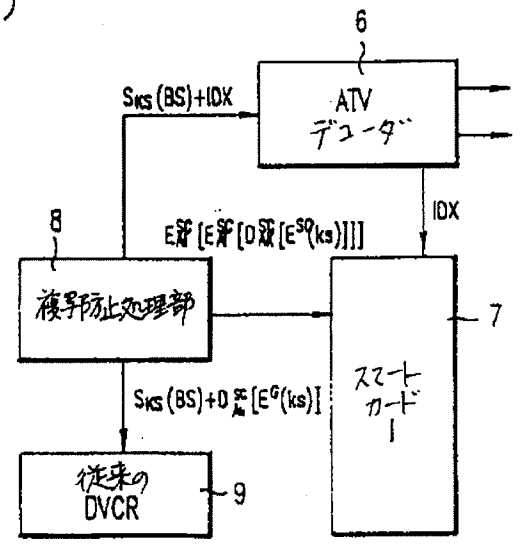

S101
入力："BS" or
"SKS(BS)+E^G(KS)"
"SKS(BS)+IDX"
S102
"SKS(BS)+IDX"?
No
Yes
S105
複写防止処理部
から；E^SC_AK[E^G(ks)]
暗号化アルゴリズム
(E^SC_AK(・))
認証キー
Ak(ROMから)
S106
DVCR(録画)に

【図１８】

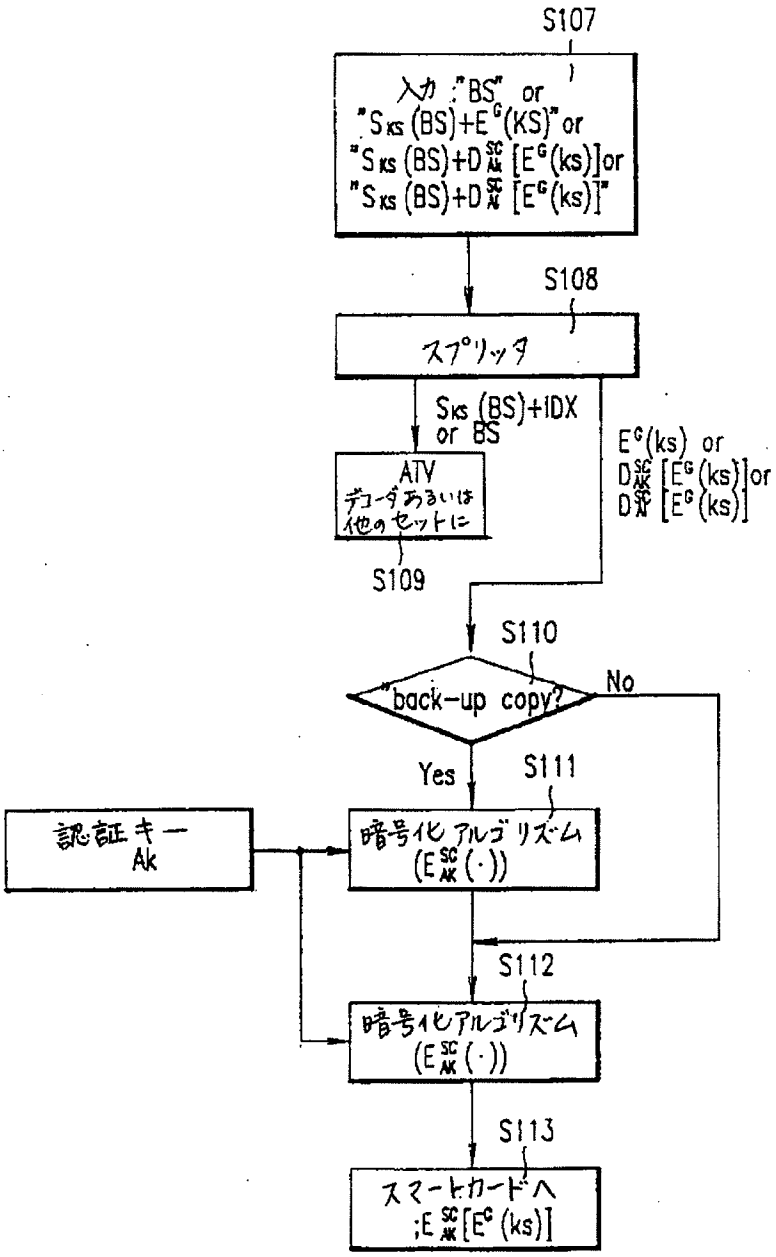
(a)


2
ATV
デコーダ
SKS(BS)+IDX
KS
IDX
4
複写防止処理部
3
スマート
カード
k
従来の
DVCR
5

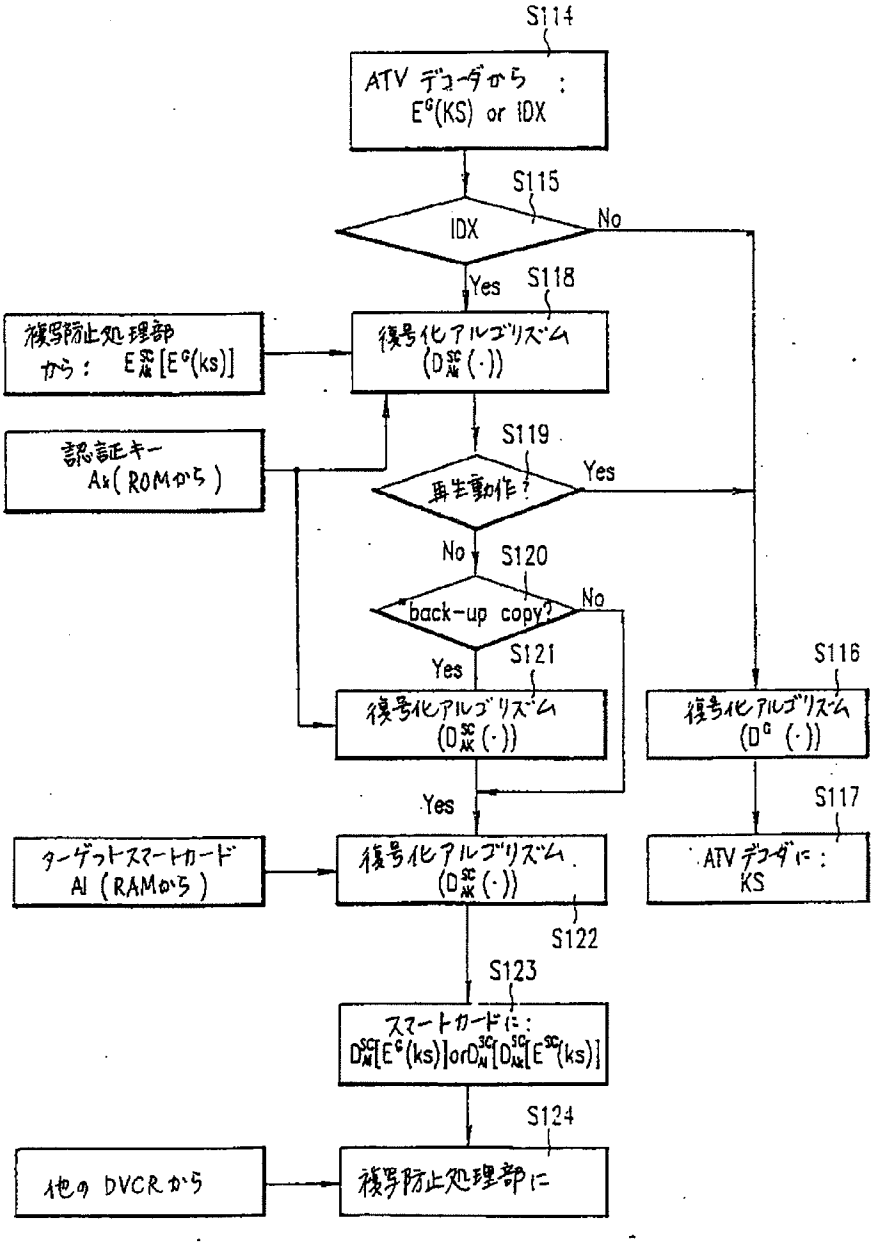
(b)


6
ATV
デコーダ
SKS(BS)+IDX
IDX
8
複写防止処理部
7
スマート
カード
1
従来の
DVCR
9

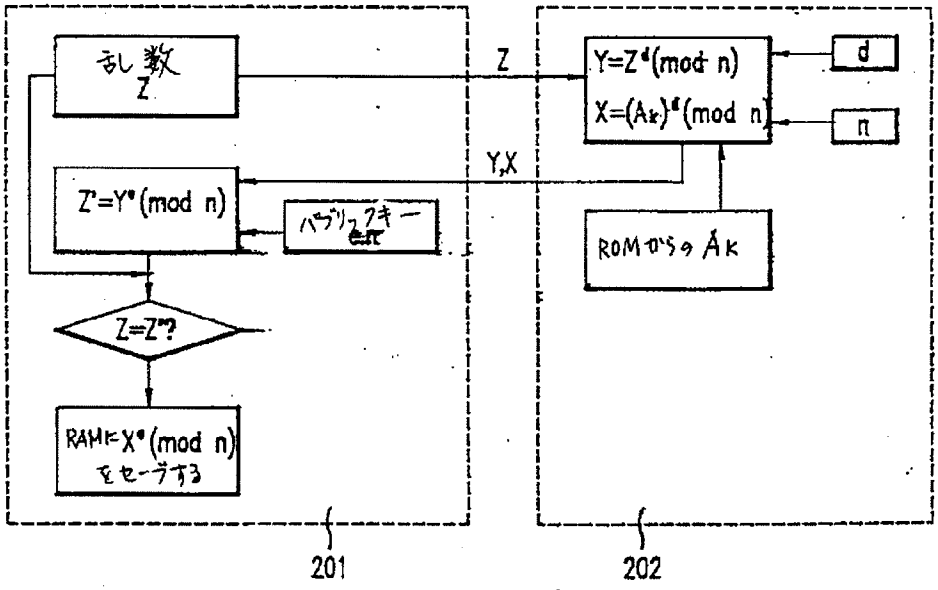
【図２０】


S107
入力："BS" or
"$S_{KS}(BS)+E^{G}(KS)$" or
"$S_{KS}(BS)+D^{SC}_{AK}[E^{G}(ks)]$ or
"$S_{KS}(BS)+D^{SC}_{AK}[E^{G}(ks)]$"
S108
スプリッタ
$S_{KS}(BS)+IDX$
or BS
$E^{G}(ks)$ or
$D^{SC}_{AK}[E^{G}(ks)]$ or
$D^{SC}_{AK}[E^{G}(ks)]$
ATV
デコーダあるいは
他のセットに
S109
S110
"back-up copy?
No
Yes
S111
認証キー
Ak
暗号化アルゴリズム
$(E^{SC}_{AK}(\cdot))$
S112
暗号化アルゴリズム
$(E^{SC}_{AK}(\cdot))$
S113
スマートカードへ
$;E^{SC}_{AK}[E^{G}(ks)]$

【図２１】


S114
ATV デコーダから：
$E^G(KS)$ or IDX
S115
IDX
No
Yes
S118
複号防止処理部
から： $E^{SC}_{AK}[E^G(ks)]$
復号化アルゴリズム
$(D^{SC}_{AK}(\cdot))$
認証キー
Ak（ROMから）
S119
再生動作?
Yes
No
S120
back-up copy?
No
Yes
S121
S116
復号化アルゴリズム
$(D^{SC}_{AK}(\cdot))$
復号化アルゴリズム
$(D^G(\cdot))$
S117
Yes
ターゲットスマートカード
AI（RAMから）
復号化アルゴリズム
$(D^{SC}_{AK}(\cdot))$
ATV デコーダに：
KS
S122
S123
スマートカードに：
$D^{SC}_{AI}[E^G(ks)]$ or $D^{SC}_{AI}[D^{SC}_{AK}[E^{SC}(ks)]]$
S124
他の DVCR から
複号防止処理部に

【図２２】


乱数
Z
Z
Y=Z^d(mod n)
X=(Ak)^d(mod n)
d
n
Y,X
Z'=Y^e(mod n)
パブリックキー
ROMからのAk
Z=Z'?
RAM←X^e(mod n)
をセーブする
201
202